

NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA



THESIS

INTERNETWORKING: RECOMMENDATIONS ON NETWORK MANAGEMENT FOR K-12 SCHOOLS

by

Dennis Michael Trepanier
September 1995

Thesis Advisor:
Associate Advisor:
Second Reader:

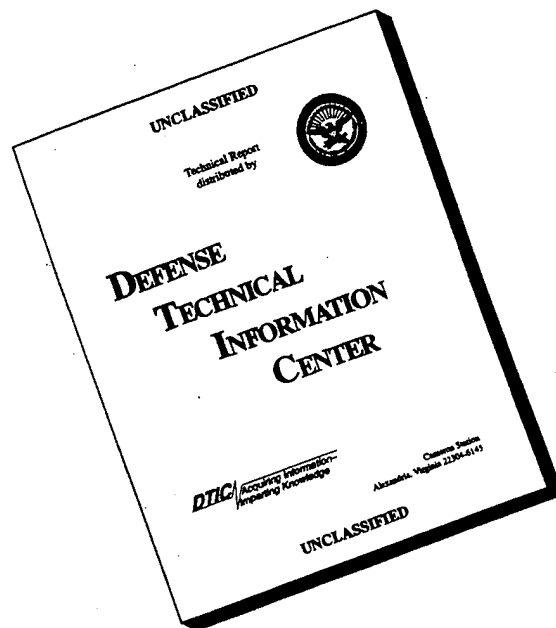
Don Brutzman
Myung W. Suh
Rex Buddenberg

Approved for public release; distribution is unlimited.

DTIC QUALITY INSPECTED 1

19960402 113

DISCLAIMER NOTICE



**THIS DOCUMENT IS BEST
QUALITY AVAILABLE. THE
COPY FURNISHED TO DTIC
CONTAINED A SIGNIFICANT
NUMBER OF PAGES WHICH DO
NOT REPRODUCE LEGIBLY.**

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 | |
|---|---|---|-------------------------------------|----------------|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503. | | | | |
| 1. AGENCY USE ONLY (Leave blank) | 2. REPORT DATE September 1995 | 3. REPORT TYPE AND DATES COVERED Master's Thesis | | |
| 4. TITLE AND SUBTITLE: INTERNETWORKING: RECOMMENDATIONS ON NETWORK MANAGEMENT FOR K-12 SCHOOLS | | 5. FUNDING NUMBERS | | |
| 6. AUTHOR Dennis Michael Trepanier | | | | |
| 7. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey CA 93943-5000 | | 8. PERFORMING ORGANIZATION REPORT NUMBER | | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER | | |
| 11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. | | | | |
| 12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited. | | 12b. DISTRIBUTION CODE | | |
| 13. ABSTRACT <p>Telecommunications network technology can enrich both classrooms and administration of the nation's public schools in preparation for the global economy of the 21st century. Shortages of curricula and reference materials may no longer be problems as up-to-date materials, guest educators, and people at otherwise inaccessible locations are brought directly into the learning environment. Teachers and administrators will work in new ways with their colleagues across the nation and around the world. A critical and seldom recognized requirement to support the day-to-day operation of educational telecommunications networks is sustainable network management.</p> <p>This study describes network management, services, and associated tools essential to the proper operation of networks in the kindergarten through twelfth grade (K-12) educational mission. It also discusses network management solutions that educators and others can use to optimize network technology. Case studies are presented which compare different networks, their tools, and approaches to management. Recommendations for sustainable K-12 network management and regional action are provided based upon analysis of the literature and these cases.</p> | | | | |
| 14. SUBJECT TERMS Telecommunication Networks, Network Management, Monterey Bay Network, K-12 education, Network Administration, Network Operating Center (NOC), Network Information Center (NIC) | | | 15. NUMBER OF PAGES | 16. PRICE CODE |
| 17. SECURITY CLASSIFI- CATION OF REPORT Unclassified | 18. SECURITY CLASSIFI- CATION OF THIS PAGE Unclassified | 19. SECURITY CLASSIFI- CATION OF ABSTRACT Unclassified | 20. LIMITATION OF ABSTRACT UL | |

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)

Prescribed by ANSI Std. Z39-18 298-102

Approved for public release; distribution is unlimited.

**INTERNETWORKING:
RECOMMENDATIONS ON NETWORK MANAGEMENT
FOR K-12 SCHOOLS**

Dennis M. Trepanier
Lieutenant Commander, United States Navy
B.A., Northwest Nazarene College, 1977

Submitted in partial fulfillment
of the requirements for the degree of

**MASTER OF SCIENCE
IN
INFORMATION TECHNOLOGY MANAGEMENT**

from the

NAVAL POSTGRADUATE SCHOOL

September 1995

Author:

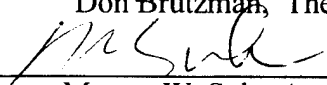


Dennis Michael Trepanier

Approved by:



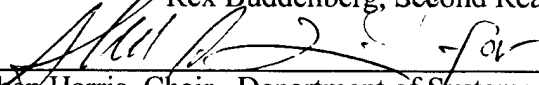
Don Brutzman, Thesis Advisor



Myung W. Suh, Associate Advisor



Rex Buddenberg, Second Reader



Reuben Harris, Chair, Department of Systems Management

ABSTRACT

Telecommunications networking technology can enrich both classrooms and administration of the nation's public schools in preparation for the global economy of the 21st century. Shortages of curricula and reference materials may no longer be problems as up-to-date materials, guest educators, and people at otherwise inaccessible locations are brought directly into the learning environment. Teachers and administrators will work in new ways with their colleagues across the nation and around the world. A critical and seldom recognized requirement to support the day-to-day operation of educational telecommunications networks is sustainable network management.

This study describes network management, services, and associated tools essential to the proper operation of networks in the kindergarten through twelfth grade (K-12) educational mission. It also discusses network management solutions that educators and others can use to optimize network technology. Case studies are presented which compare different networks, their tools and approaches to management. Recommendations for sustainable K-12 network management and regional action are provided based on analysis of the literature and these cases.

TABLE OF CONTENTS

| | |
|---|----|
| I. INTRODUCTION..... | 1 |
| A. OVERVIEW | 1 |
| B. BACKGROUND | 3 |
| C. MOTIVATION | 8 |
| D. THESIS ORGANIZATION | 12 |
| 1. Chapter Descriptions..... | 12 |
| 2. How to Use this Thesis | 13 |
| a. Policy Makers, Administrators, Board of Education Members. | 13 |
| b. Educators and Local School Network Managers | 14 |
| c. Parents | 14 |
| d. Network Managers and Administrators | 14 |
| e. Researchers and Networking students | 15 |
| E. SUMMARY | 15 |
| II. RELATED WORK | 17 |
| A. INTRODUCTION | 17 |
| B. MONTEREY BAYNET AND K-12 NETWORKS | 17 |
| 1. Monterey BayNet / I ³ LA Projects | 18 |
| 2. K-12 Schools and the Internet | 20 |

| | |
|---|----|
| 3. References for Information on the Internet | 22 |
| C. NETWORK MANAGEMENT REFERENCES | 23 |
| 1. Hardcopy References | 23 |
| 2. On line Resources on Network Management | 23 |
| D. SUMMARY | 24 |
| III. PROBLEM STATEMENT | 27 |
| A. INTRODUCTION | 27 |
| B. PROBLEM STATEMENT | 27 |
| C. SUMMARY | 30 |
| IV. NETWORK MANAGEMENT MODELS | 33 |
| A. INTRODUCTION | 33 |
| B. USER REQUIREMENTS | 33 |
| C. MODELS | 35 |
| 1. Structural Model | 35 |
| 2. System Life Cycle Model | 39 |
| 3. Open System Interconnection (OSI) Functional Model | 41 |
| a. Fault Management | 42 |
| b. Accounting Management | 42 |
| c. Configuration and Name Management | 43 |

| | |
|---|----|
| d. Performance Management | 43 |
| e. Security Management | 44 |
| D. SUMMARY | 44 |
| V. CAPACITY AND RELIABILITY PLANNING | 47 |
| A. INTRODUCTION | 47 |
| B. CAPACITY PLANNING | 47 |
| C. RELIABILITY | 50 |
| D. SUMMARY | 52 |
| VI. NETWORK OPERATING CENTER (NOC) FUNCTIONS | 53 |
| A. INTRODUCTION | 53 |
| B. FAULT MANAGEMENT | 54 |
| 1. Network Monitoring Display | 54 |
| 2. Network Faults, Fault Identification and Isolation | 60 |
| 3. Alarm Generation and Threshold Definition | 62 |
| 4. Alarm Processing | 63 |
| 5. Trouble Ticketing | 63 |
| 6. Troubleshooting Tools | 65 |
| C. NETWORK ACCOUNTING MANAGEMENT | 71 |
| 1. Reasons for Network Accounting. | 71 |

| | |
|---|-----|
| 2. Network Cost Sharing and Cost Accounting. | 74 |
| 3. Other Uses of Network Accounting Information | 78 |
| D. CONFIGURATION AND NAME MANAGEMENT | 79 |
| 1. Configuration Parameters | 80 |
| 2. Name Management | 87 |
| E. PERFORMANCE MANAGEMENT | 90 |
| 1. Performance Monitoring | 92 |
| 2. Operational Monitoring | 95 |
| a. Simple Network Management Protocol (SNMP) | 96 |
| b. Operational Limitations of SNMP. | 101 |
| 3. Operational Management Reports | 104 |
| F. SECURITY MANAGEMENT | 105 |
| 1. Network Security Management | 106 |
| 2. Deciding on the Degree of Network Security | 106 |
| 3. SNMPv2 (version 2) | 109 |
| G. SUMMARY | 110 |
| VII. NETWORK INFORMATION CENTER (NIC) FUNCTIONS | 113 |
| A. INTRODUCTION | 113 |
| B. CONNECTION SERVICES | 113 |
| 1. Internet Service Connections | 113 |

| | |
|---|-----|
| 2. Dial-in Service | 114 |
| a. Serial Line Internet Protocol (SLIP) | 115 |
| b. Point-to-Point Protocol (PPP) | 115 |
| C. OTHER NETWORK SERVICES | 116 |
| 1. Domain Name System (DNS) | 117 |
| 2. Mail | 121 |
| 3. Network News | 124 |
| 4. Network Time | 126 |
| 5. World Wide Web (WWW) Service | 127 |
| 6. Documentation and Training | 128 |
| a. <i>telnet</i> | 128 |
| b. <i>ftp</i> (File Transfer Protocol) | 129 |
| c. Electronic Mail | 129 |
| d. Other Network Information Center (NIC) Services | 130 |
| D. SUMMARY | 131 |
| VIII. NETWORK OPERATIONS EXAMPLE CASES AND ANALYSIS | 133 |
| A. INTRODUCTION | 133 |
| B. EXAMPLE CASES | 133 |
| 1. NASA Science Internet (NSI) Operations | 133 |
| a. Background | 133 |

| | | |
|-----|---|-----|
| b. | Network Description | 135 |
| c. | Staffing | 138 |
| 2. | California State University Network (CSU NET) | 139 |
| a. | Background | 140 |
| b. | Network Description | 140 |
| c. | Staffing | 141 |
| 3. | Energy Sciences Network (ES NET) | 142 |
| a. | Background | 142 |
| b. | Network Description | 143 |
| c. | Staffing | 149 |
| C. | NETWORK MANAGEMENT SYSTEM ANALYSIS | 149 |
| D. | SUMMARY | 153 |
| IX. | CONCLUSIONS AND RECOMMENDATIONS | 155 |
| A. | CONCLUSIONS | 155 |
| B. | RECOMMENDATIONS | 156 |
| 1. | Conformance to Standards | 157 |
| 2. | Network Management Protocol | 157 |
| 3. | Network Management System (NMS) | 158 |
| 4. | Staffing | 159 |
| 5. | Reports | 160 |

| | |
|--|-----|
| 6. Accounting | 161 |
| C. RECOMMENDATIONS FOR FUTURE WORK | 161 |
| D. SUMMARY | 162 |
| LIST OF REFERENCES | 165 |
| APPENDIX A | 173 |
| INITIAL DISTRIBUTION LIST | 177 |

LIST OF FIGURES

| | |
|---|----|
| 1.1. Key elements of network management. | 2 |
| 1.2. Emerging needs of K-12 schools. | 3 |
| 1.3. Monterey BayNet ATM, Frame Relay, and ISDN Tiered Sites | 5 |
| 1.4. Monterey BayNet, topographical network map - Monterey County. | 6 |
| 1.5. Monterey BayNet, topographical network map - Santa Cruz County | 7 |
| 1.6. Focus of initial network planning efforts. | 8 |
| 1.7. Agenda for Education in California | 10 |
| 3.1. Problem statement, present and future research questions | 31 |
| 4.1. Network management requirements for Monterey BayNet | 34 |
| 4.2. Structural model of network management | 36 |
| 4.3. Modified Structural model of network management applied to Monterey BayNet | 37 |
| 4.4. System Life-Cycle model of network management | 39 |
| 4.5. Functional tasks of the System Life-cycle model | 40 |
| 4.6. OSI management functional model of network management | 41 |
| 5.1. Decisions affected by capacity planning | 48 |
| 5.2. Capacity relief methods | 49 |
| 5.3. Measures of reliability | 51 |
| 5.4. Methods to increase net work reliability | 51 |
| 6.1. Goals of network fault management | 54 |

| | |
|---|----|
| 6.2. Geographic network map, world | 56 |
| 6.3. Site topological network map | 57 |
| 6.4. Network link view map | 58 |
| 6.5. Equipment view | 59 |
| 6.6. Categories of network faults | 60 |
| 6.7. Symptoms of connectivity errors | 61 |
| 6.8. Examples of network agent events | 62 |
| 6.9. Events display | 64 |
| 6.10. PING features | 68 |
| 6.11. TRACEROUTE to Antarctica | 69 |
| 6.12. NSLOOKUP examples | 70 |
| 6.13. Reasons for network accounting | 72 |
| 6.14. Additional reasons for network accounting | 72 |
| 6.15. Network accounting information | 73 |
| 6.16. Fixed, variable, and total cost | 76 |
| 6.17. Deterrents to usage reporting | 78 |
| 6.18. Router configuration methods | 85 |
| 6.19. Configuration parameters | 86 |
| 6.20. Hostname registration and assignment | 89 |
| 6.21. Performance management activities | 91 |
| 6.22. Internet growth | 97 |

| | |
|--|-----|
| 6.23. SNMP key elements | 98 |
| 6.24. SNMP architecture | 99 |
| 6.25. Limitations of SNMP | 102 |
| 6.26. CERFnet weekly network summary report format | 104 |
| 6.27. NASA Science Internet (NSI) report formats. | 105 |
| 6.28. Components of network security management. | 107 |
| 6.29. SNMPv2 improvements. | 110 |
| 7.1. Domain Name System (DNS) Architecture | 119 |
| 7.2. Reasons to get a Domain Name Server | 120 |
| 7.3. Simple Mail Transfer Protocol (SMTP) | 122 |
| 7.4. Steps to become a USENET News Site.. . . . | 125 |
| 7.5. Setting up a Web server | 128 |
| 8.1. NASA Science Internet (NSI) world network map | 134 |
| 8.2. NASA Science Internet - U.S. network map | 136 |
| 8.3. Energy Sciences network (ESnet) - U.S. network map | 144 |
| 8.4. ESnet exponential growth | 145 |
| 8.5. ESnet Network Operating Center (NOC). | 147 |
| 8.6. Network Management System Evaluation Criteria | 150 |
| 9.1. National Research and Education Network (NREN) - Internet | 163 |

LIST OF TABLES

| | |
|---|----|
| 6.1. Icon and Link dynamic display color scheme | 60 |
| 6.2. Event number vs. event descriptions | 63 |
| 6.3. Network protocols | 81 |
| 6.4. Routing protocols | 83 |
| 6.5. Top level domains | 88 |
| 6.6. Relative speeds of an e-mail message | 92 |

ACKNOWLEDGEMENTS

I wish to acknowledge the support and encouragement of my wife Mary, and children, Rick & his wife Pauline, Jennifer(9), Natalie(7) and Denise(2). I also thank the following individuals for patient explanations and assistance in gathering information for use in this document.

First and foremost, I wish to express gratitude to Professor Don Brutzman, my primary thesis advisor, for his steady guidance and his zeal for the Internet. Without his vision and involvement in Monterey BayNet, this project would not have been possible. I also thank Professor Myung Suh, Rex Buddenberg, Dave Norman of the Naval Postgraduate School Computer Center, Tony Hain of Energy Sciences Network (ESnet) operations, Jeanine Kamerdze of NASA Science Internet (NSI) operations, Mike Marcinkevicz and Jim Patterson of CSUnet, and Chris Taylor of California State University, Monterey Bay (CSUMB), who have provided wisdom, insight, and a wealth of experience, each from his own unique perspective.

I would like to acknowledge the tremendous support of Nancy Giberson and Rowland Baker at the Santa Cruz County Office of Education, and Mike Mellon and Mike Herbst of the Monterey County Office of Education for giving us the latitude to have fun while we were putting our pieces of Monterey BayNet together. Last (but not least!) I want to express appreciation to Kam Matray, who I call the "champion" of our Monterey BayNet K-12 network. She has been among our strongest advocates and we are fortunate to have her.

I. INTRODUCTION

A. OVERVIEW

Today's telecommunications networks are dynamic information flow systems that can move digital information from raw binary form or simple ASCII text through high-fidelity audio and full-motion video at enormous data rates. Electronic messaging systems such as electronic mail (e-mail) can send correspondence to almost any location in the world in a flash without human intervention, using network methodologies that are completely transparent to users (Schatt 92).

In spite of all these virtues, such "transparency" can be deceiving. Today's sophisticated telecommunications networks handle data rapidly and automatically, but are also vulnerable to instantaneously changing environmental conditions that may degrade or terminate their performance. In cases where operation of the network is critical to the function of an organization, network outages are very costly and can result in significant losses in time, money and effort.

To ensure optimum reliability, continuous performance and sustainable future growth, networks must be managed (Schatt 92). Unfortunately network management has lagged behind the technical advances in other areas of networking, primarily because of lack of definition and standardization.

One of the several reasons network management has lagged behind other areas of open networking is that there is a lack of agreement about what network management is. While there is no shortage of literature offering platitudes about the five functional areas of network network management -

fault, configuration, accounting, performance, and security management - the body of literature offering practical details about managing real open networks has, until recently, been virtually nonexistent. (Lynch, Rose 93)

Network management has many different definitions and models, but ultimately consists of two basic elements, *monitoring* and *control* (RFC 1021).

- | |
|---|
| <ul style="list-style-type: none">● Monitoring - knowing the current status and parameters of the network● Control - the ability to change something about the network |
|---|

Figure 1.1 Key Elements of Network Management (RFC 1021)

To facilitate these two functions, a network management station called a Network Operating Center (NOC) is used. The NOC contains hardware, software, communication, and staffing to monitor and control the network. Another function of network management, the Network Information Center (NIC), deals more directly with helping end users by providing a help desk, administrative support, and information services.

Whatever model of network management is chosen, the model (or combination of models) needs to be tailored to fit the needs of K-12 schools. Those needs are changing and steadily evolving. The "information revolution" of the Internet is continuously changing the availability of information. K-12 schools deserve a variety of tools to educate children and pave their way to adulthood in a competitive world, where their success may depend on the information they can access and employ.

The emerging needs of K-12 schools can be found in *Building the Future - K-12 Network Technology Planning Guide* (California Department of Education 94), summarized in Figure 1.2.

- teacher training and support
- school and district planning for integration of telecommunications into instruction and administration
- time in the school schedule for professional and student learning activities
- effective assessment measures
- financial support
- multiple phone lines or local area networks

Figure 1.2 Emerging needs of K-12 Schools (California Department of Education 94)

This thesis builds on the work in a related thesis, "*Internetworking: Implementing a Wide-Area Network (WAN) for K-12 Schools*" (Bigelow 95). This thesis explores various cases in network management for practical and economic solutions to managing a sustainable regional research and education information network. It is written from the perspective of educators and administrators in K-12 schools. Finally it provides K-12 network implementors and network technology mentors recommendations in making network management decisions.

B. BACKGROUND

Monterey BayNet is a Wide-Area Network (WAN) connecting public schools at grades Kindergarten through twelfth grade (K-12), as well as other educators and research institutions in Monterey and Santa Cruz counties on the central California coast. The emerging network is the ongoing product of two years of collaborative work and

volunteer efforts from individuals, researchers, and businesses throughout the community spearheaded by an organization named I³LA (Initiative for Information Infrastructure and Linkage Applications) (Bigelow 95)(Brutzman 94, 95).

Implementation of the network was facilitated by a grant awarded to the I³LA consortium from California Research and Education Network (CalREN) in April 1994. The grant provides funding from Pacific Bell for telecommunications service (free wide-area connectivity) to fourt-three I³LA "test bed" school sites through June of 1996. CalREN was initiated by Pacific Bell to fund projects that advance telecommunications technologies and information infrastructure (PacBell 94).

A key decision was made early in the Monterey BayNet project to use Frame Relay as the core networking technology primarily because it offered a wide selection of bandwidths from 56Kbps up to 1.55 Mbps (T1). Frame relay is suitable for the present and foreseeable data needs of most K-12 schools. Figures 1.4 and 1.5 are topological network maps of Monterey BayNet in Monterey and Santa Cruz Counties, respectively. Allowances were made in the design of the network for the additional connection of Integrated Data Services Network (ISDN) services to a limited number of schools.

Finally, the network also has an Asynchronous Transfer Mode (ATM) high-speed network (at 55 to 155 Mbps) between "Tier I" sites, to complete a three-tier structure (Figure 1.3). Tier I ATM-level sites employ multiple very high-bandwidth information streams such as video, audio, and 3D computer graphics. Tier II sites are sites that were expected to employ moderately high bandwidth (i.e. Frame Relay). Tier III sites are

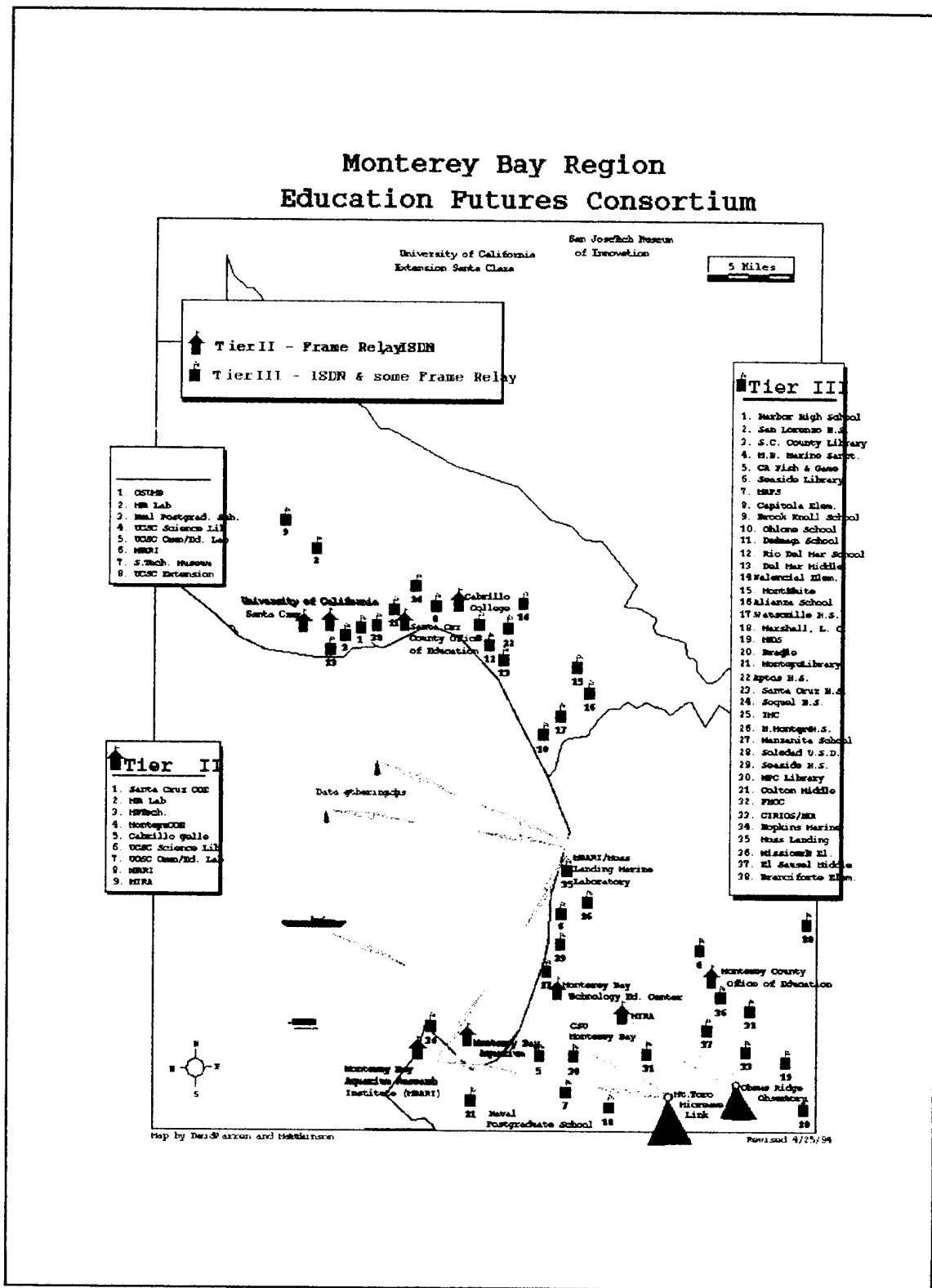
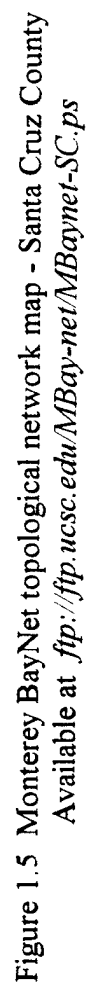


Figure 1.3 Monterey BayNet ATM, Frame Relay, ISDN Tiered Sites



schools and libraries with high-bandwidth ATM connectivity, often in addition to conventional T1 connections with bandwidth adequate to meet their information needs and a single video channel (Brutzman 94).

C. MOTIVATION

Monterey BayNet was designed and implemented through the efforts of the I³LA consortium. A long-term goal of I³LA was to create a *sustainable* regional information infrastructure that can function as a community resource and provide full access to the Internet at a variety of bandwidth rates (Bigelow 95). Sustainability is not yet assured. Most of the planning effort during the first stages of network development focused on requirements listed in Figure 1.6 to establish initial connectivity.

- funding resources
- selection and procurement of standard hardware items (routers, CSU/DSU)
- site selection, inspections, and installations
- network domain names and addressing
- network and equipment configurations
- network application software installation.

Figure 1.6 Focus of Initial Network Planning Efforts (Bigelow 95)

Until the spring of 1995, when approximately half of the 43 test bed sites were on line, not much attention was addressed to the issue of how to manage the network. This was due to concentration of efforts on the many challenges associated with installing a new network. As more sites became connected, more issues and questions were raised than the existing cadre of volunteers could answer. When network problems or site

outages occurred, the lack of corrective measures and experienced personnel resources was a serious problem. Clearly, for the network to be a sustainable regional information infrastructure, it must be managed. Volunteer efforts alone (at least at this stage in the development) are not enough.

The mission of the California education system supports justification for implementing a K-12 regional telecommunication network. The California State Department of Education's mission statement (Figure 1.7) is called the "Agenda for Education in California" (Eastin 95). These principles are reiterated and elaborated in *Building the Future - K-12 Network Technology Planning Guide* (California Department of Education 94). It is important to note that Monterey BayNet has direct applicability pertaining to each point in the Agenda for Education in California. These points are now examined in detail.

Supporting the first point in Figure 1.7, Monterey BayNet will increase parent involvement in many ways. Parents can access student and educator World-Wide Web (WWW) homepages and communicate with teachers via e-mail. Businesses gain opportunities to "enter the classroom environment" with their new technology. The electronic information network will enable the creation of community "people networks" and support school sites with better access to information.

To support the second point in Figure 1.7, increased availability of information

1. BROADEN THE BASE OF SUPPORT FOR EDUCATION
 - increase parent involvement.
 - strategically partner with business.
 - create community networks supporting school sites.
2. INCREASE LOCAL CONTROL OVER DECISIONS
 - encourage site-based management.
 - reduce the education code.
 - reduce administrative requirements.
3. FOCUS OUR EFFORTS ON RESULTS, NOT PROCESS, BY DEVELOPING STANDARDS TO MEASURE PROGRESS
 - develop grade level proficiency standards.
 - develop content and performance measurements.
 - ensure that every child is a reader.
4. PREPARE A SKILLED WORKFORCE
 - create partnerships to provide opportunities for all students, college-bound and non-college-bound.
 - strive for multilingual training for all students.
 - establish lifelong positive learning patterns for all children beginning with preschool.
5. ENSURE THAT FACILITIES AND TECHNOLOGY ARE EXCELLENT
 - expand partnerships with businesses, unions, communities, and the public sector (military, higher education, etc.) to equip schools and students with up-to-date technology and facilities.
 - ensure that all schools are clean, well lighted, safe and up-to-date.

Figure 1.7 Agenda for Education in California (Eastin 95)

resources afforded by Monterey BayNet promotes streamlined administrative communication and allows educators to make informed decisions at progressively lower levels, down to the individual school site levels. Broadcast capabilities of networks allow sharing of a single source document with hundreds of recipients simultaneously, eliminating redundant paper copies. Hardware sharing on a network allows individuals to print documentation remotely, reducing mailing costs.

Supporting the third point, the availability of the Internet provides practice in computer literacy and an interesting, continuously changing vehicle for reading literacy for all grades. Standards to measure progress can be developed, promulgated, measured, and analyzed rapidly using telecommunication network technology. In addition, some standards that have already been researched and developed by other organizations can be readily implemented, preventing a costly repetition of research already performed.

To support the fourth point, with the arrival of the "Information Revolution" Monterey BayNet provides a method for students to exercise internetworking and prepare them for a future where computing and telecommunication skills will be a critical asset in a competitive job market. Testing the effectiveness of this approach remains an important long term educational research goal.

Supporting the last point in Figure 1.7, telecommunications networks provide access to the most current information, using the most up-to-date technologies. Moreover, with the variety of alternate sources of information on the Internet and other

network resources, it becomes easier to affirm the validity and importance of that information.

D. THESIS ORGANIZATION

This thesis is tailored for technical and non-technical readers. A short description of each chapter of this thesis is provided below as an overview:

1. Chapter Descriptions

- **CHAPTER 1 - INTRODUCTION** - Contains an overview of network management, how it applies to K-12 schools, and motivation for this thesis.
- **CHAPTER 2 - RELATED WORK** - Describes current projects that are affiliated with Monterey BayNet, informative hardcopy and on line references on Monterey BayNet, K-12 Schools, the Internet, and network management.
- **CHAPTER 3 - PROBLEM STATEMENT** - Clearly defines the problem of identifying what it will take to make Monterey BayNet sustainable and suggesting network management as a solution.
- **CHAPTER 4 - NETWORK MANAGEMENT MODELS** - Uses various different network management models to clarify the multi-faceted definition of sustainable network management.
- **CHAPTER 5 - CAPACITY AND RELIABILITY PLANNING**- demonstrates how decisions on capacity and reliability affect future decisions in building the network, including network management systems and protocols.
- **CHAPTER 6 - NETWORK OPERATING CENTER FUNCTIONS (NOC)**- Describes the composition of a NOC, how and why it is essential to the successful operation and sustainability of Monterey BayNet.

- CHAPTER 7 - NETWORK INFORMATION CENTER FUNCTIONS (NIC)
Describes the composition of a NIC, how and why it is essential to the optimum employment of Monterey BayNet.
- CHAPTER 8 - NETWORK OPERATIONS EXAMPLE CASES - Presents three cases of operating networks and a comparative analysis of the major network management systems.
- CHAPTER 9 - CONCLUSIONS AND RECOMMENDATIONS-Summarizes the importance of network management to the sustainability of Monterey BayNet and provides direction and recommendations on key sustainability issue.

2. **How to Use this Thesis**

Because there are so many aspects of network management, it can involve individuals in many different positions for its implementation. Recommendations on how to use this thesis for different individuals follow.

a. Policy Makers, Administrators and Board of Education Members

These individuals are involved in making policies on security, acceptable use, chargeback mechanisms, inter-operability, reliability and standardization and other issues that must be faced in implementing and sustaining Monterey BayNet. This thesis demonstrates the need for network management policy formulation and provides support, guidance, and authoritative references for those policies.

b. Educators and Local School Network Managers

Since these individuals are involved in using and maintaining the networks, this thesis can provide them a better understanding of how their local information systems and networks interact with other network components and the Internet. A discussion of basic network troubleshooting tools can provide them with an understanding sufficient to perform limited diagnostics to assist in troubleshooting and fault localization. It also provides a basic understanding of the network applications and services provided by the Network Operating Center (NOC) and Network Information Center (NIC).

c. Parents

Parents can benefit from this thesis by gaining an understanding of telecommunications networks, network management, the nature of the information revolution, and how Monterey BayNet can support and enhance the education of their children.

d. Network Managers and Administrators

Network Managers and administrators can use the information provided in this thesis as a starting point on the design of a Network Operating Center and Network Information Center. It can also be used to demonstrate the need for Network Management tools to the policy makers, and those that make budgeting and resource allocation decisions.

e. Researchers and Networking Students

Researchers and Networking students can benefit from this thesis by using it for the broad understanding of Network Management that it presents. It can provide a base for more in-depth research in a multitude of interesting areas. Some suggested topics for in-depth analysis are presented in chapter 9, section C, "Recommendations for Future Work". Researchers on projects outside of Monterey BayNet can use the thesis to gain an understanding of how network management and Monterey BayNet can help disseminate the results of their research and findings for the benefit of K-12 students in Monterey County, Santa Cruz County and throughout the World.

E. SUMMARY

Telecommunications networks provide an unprecedented access to information and can be used to convey information to students as well as to educate them in creating, obtaining, displaying, conveying and storing information. Networks are becoming increasingly essential in a world with a growing global economy. K-12 schools need tools that prepare students for adulthood in a competitive world. The versatile nature of Monterey BayNet in promoting the Agenda of Education for California makes it an asset worthy of investment and sustainable support.

II. RELATED WORK

A. INTRODUCTION

This chapter discusses works and references related directly to the inception and implementation of Monterey BayNet. Some are published and others can be found on the World-Wide Web (WWW). Related works on collaborative education and research in the Monterey Bay area, K-12 schools and the Internet, the Internet itself, and network management are also listed.

The majority of written correspondence in the building of Monterey BayNet remains unpublished. A large amount of corporate knowledge was gained over the Internet and through the utilization of an e-mail list server provided by Monterey Bay Aquarium Research Institute (MBARI). The list server provided this group effort a large amount of leverage and convenience in communicating to anyone who subscribed. Group training sessions, meetings and agendas, current events, hardware and software tips, and network status were all shared over the list server.

Since this thesis builds on the work of Jon Bigelow in his thesis *Internetworking: Planning and Implementing a Wide-Area Network (WAN) for K-12 Schools* (Bigelow 95), some of the related works below also appear in his thesis.

B. MONTEREY BAYNET AND K-12 NETWORKS

There are many published references directly applicable to building and implementing telecommunications networks in the K-12 educational field. The Internet

contains references to government agency, business, and organization efforts and contributions to K-12 schools nationwide. Of these references, those most applicable to Monterey BayNet are listed and described here.

1. Monterey BayNet / I³LA Projects

- *Networked Ocean Science Research and Education, Monterey Bay California* (Brutzman 95). An overview of the research effort of I³LA (Monterey BayNet) around a common theme of environmental and ocean science. Key areas of action are listed and amplified: connectivity, content, access and applications. To subscribe to the I³LA listserver, e-mail a message **help** to *Majordomo@mbari.org* for a list of commands.

- *I³LA Net Design White Paper* (Brutzman 94). The White Paper is the first document that combines several Monterey Bay regional initiatives into a single focused purpose. It is, in essence, the mission and vision of I³LA that embodies the creation of a regional telecommunications network to bring an understanding and appreciation of environmental issues.

- *Internetworking: Planning and Implementing a Wide-Area Network (WAN) for K-12 Schools* (Bigelow 95). Master's thesis documenting the design and implementation of Monterey BayNet, a regional Wide-Area Network (WAN) connecting K-12 schools, research institutions, and universities throughout the Monterey Bay Area.

- *The I3LA Network: Physical Configuration Team Project* (Trepanier et al. 95).

A report created by a team of Naval Postgraduate School students which describe the efforts of a Tier I Monterey BayNet site in technology transfer to Tier II and III sites. The team's effort was successful configuring equipment and conducting end-user training.

- The I³LA home page provides access to I3LA summary information, proposals and anonymous ftp server. In addition it has many useful links to information sources on commerce, digital libraries, education, environment, government, National Information Infrastructure (NII), networking and telecommunications. Available at <ftp://taurus.cs.nps.navy.mil/pub/i3la/i3la.html>

- The Learning About Monterey Bay (LAMBAY) home page provides information about the collaborative education and research surrounding Monterey Bay. Particular emphasis is placed upon the region's diverse habitats, including the unusual marine life of the deep sea canyon (Atkinson 95). Links are provided to local education, research, libraries, and government sites. Available at <http://lambay.cse.ucsc.edu/mb>

- The Monterey Bay Regional Education Futures (MBReEF) Consortium home page provides links to information sources throughout the Monterey Bay region. Included are links referenced by region, environment, education, research, libraries, government, commerce, tourism and culture. Available at <http://www.ucsc.edu/mbay-region>

- *Real-time Environmental Information Network and Analysis System (REINAS).*

A joint project of the Baskin Center of the University of California, Santa Cruz (UCSC), Naval Postgraduate School (NPS), Monterey Bay Aquarium Research Institute (MBARI), and the National Oceanic and Atmospheric Administration Center for Ocean Analysis and Prediction (NOAA/COAP). REINAS is a distributed database environment supporting real-time and retrospective regional scale environmental science. It uses the Internet through wireless and leased-line SLIP links to achieve real-time connectivity between instrumented sites. The REINAS Project is funded by the Office of Naval Research under a University of California Santa Cruz Research Initiative (Risen 95). Available at <http://csl.cse.ucsc.edu/reinas.html>

2. K-12 Schools and the Internet

- Building the Future: K-12 Network Technology Planning Guide. The California Department of Education's statewide networking standards (California Department of Education 94). This document was carefully designed to provide thorough guidance to K-12 institutions regarding the deployment of information technology. The guide clearly defines the need for Internet access throughout the K-12 community and the educational benefits that access will yield to teachers, students and society. It also contains a comprehensive appendix on acceptable use policies (AUP), which address most concerns regarding K-12 student access to potentially objectionable material.

● The Internet Engineering Task Force (IETF). The IETF is a volunteer group that "provides a forum for working groups to coordinate technical developments of new protocols" (RFC 1718). It is the protocol engineering, development, and standardization arm of the Internet Architecture Board (IAB). Its most important function is "the development and selection of standards within the Internet protocol suite" (RFC 1718). The famous credo of the IETF, written by Dave Clark in 1992, reveals a passion for proven standards (as opposed to dictated standards), "We reject kings, presidents, and voting. We believe in rough consensus and running code" (Whittle 95).

One current component of the IETF is the Internet School Networking (ISN) working group. The ISN was chartered to "address issues related to the connection of primary and secondary schools worldwide to the Internet" (Seller 95). The group maintains a mailing list *isn-wg@nasa.gov*. To subscribe, send e-mail to *listmanager@nasa.gov* with the message **subscribe isn-wg** in the body of the message while leaving the subject line blank. The IETF and ISN have produced several IETF Request For Comments (RFCs) pertaining directly to K-12 Internet connectivity. They include:

- RFC 1578 FYI on Questions and Answers: Answers to Commonly Asked 'Primary and Secondary School Internet User' Questions (Sellers 94).
- RFC 1709 K-12 Internetworking Guidelines (Gargano 94).
- RFC 1746 Ways to Define User Expectations (Manning 94).

3. References for Information on the Internet

Numerous additional books exist for information on the Internet. Some notable entries include:

- *World Link: An Internet Guide for Educators, Parents, and Students* (Joseph 95).
- *Entering the World-Wide Web (WWW): A Guide to Cyberspace* (Hughes 94).
- *The Web Empowerment Book* (Abraham 94).
- *WWW Unleashed* (December 95).
- *The Whole Internet* (Krol 93).
- *Mastering the Internet* (Cady, McGregor 95)

For online IETF information and document retrieval , an IETF search page will access Requests For Comments (RFC's), Internet Standards, For Your Information (FYI documents), etc. This information provides fascinating technical information while documenting the historical events and developments in the growth of the Internet. Available at <http://www.internic.net/ds/dspg0intdoc.html>

The Internet Society (ISOC) home page is an excellent source of current research papers, conference talks, IETF meeting minutes, and other items of interest in the growth and development of the Internet. The Internet Society is the premiere organization focused on both the people and the technical side of internetworking. Membership is highly recommended. Available at <http://info.isoc.org/>

C. NETWORK MANAGEMENT REFERENCES

1. Hardcopy References

Comprehensive hard copy references for information on wide-area networks (WANs) are not as plentiful one might expect, considering the magnitude on the growth of the Internet. However, some books with notable entries include:

- *Telecommunications Network Management into the 21st Century: Techniques, Standards, Technologies and Applications* (Aidarous 94)
- *Network Management - Techniques, Tools, and Systems* (Held 92)
- *Internet System Handbook* (Lynch, Rose 93)
- *Understanding Network Management , Strategies and Solutions* (Schatt 93)
- *SNMP, SNMPv2, and CMIP, The Practical Guide to Network Management Standards* (Stallings 93)
- IBM NetView Operation Manuals (IBM 93):
 - *AIX SystemView NetView/6000 USERS GUIDE*
 - *AIX Trouble Ticket/6000 AT A GLANCE*
 - *AIX Trouble Ticket/6000 USERS GUIDE*

2. Online Resources on Network Management

The most current source of information on network management systems is the World-Wide Web (WWW) itself. Some online business resources used are:

- Cabletron SPECTRUM Network Management System
Available at <http://www.ctrn.com/Catalog/Net-Management>
- Hewlett-Packard Open View Network Management System
Available at <http://www.dmo.hp.com/nsmd/ov/main.html>

- IBM NetView Network Management System
Available at <http://www.raleigh.ibm.com/nv6/nv6prod.html>
- Novell Net Manager Network Management System
Available at <http://netwire.novell.com/SalesMkt/BuyersGuide/Section7.html>
- Racal-Datacom Network Management Systems
Available at <http://www.racal.com/racal.html>
- Solstice SunNet Network Manager
Available at <http://www.sun.com/cgi-bin/show?products-n-solutions/sw/solstice/index.body>

Reviews of Network Management Systems (NMS) by the Air Education and Training Command (AETC), Randolph Air Force Base, San Antonio, Texas and the University of Michigan can be found on the Internet. Products evaluated and ranked were HP OpenView 3.1, Sun Net Manager 2.0, IBM NetView/6000, and Cabletron SPECTRUM. The executive summary was especially useful. Also at this location are lists of Simple Network Management Protocol (SNMP) resources, an IETF catalog of network management Tools, a WWW SNMP management information base (MIB) browser, network management servers, and other network management resources.

Available at: <http://tampico.cso.uiuc.edu/~gressley/netmgmt/>

D. SUMMARY

Many works related to the vision, mission and creation of Monterey BayNet are available both in hard copy and on the Internet. With the availability of the WWW, the options for online reference material seems endless. For example, most of the graphics in this report were downloaded as .gif format graphics files from Internet web pages.

There is significant information on network management and protocols in the RFCs accessible on the Internet. Network management product comparisons and evaluations are also available. Familiarity with some of these references is highly recommended for individuals working on network management.

III. PROBLEM STATEMENT

A. INTRODUCTION

Experience has shown that building a wide-area network through community volunteer efforts and collaboration takes a great deal of dedication and energy, together with moderate material resources (Bigelow 95). The initial success of Monterey BayNet also shows that it is possible. In funding the first two years of frame relay service, the Pacific Bell CalREN grant provided motivation for participating organizations to make initial hardware purchases and install equipment sites to take advantage of the "free" PacBell frame relay service. Often decisions were made by consensus of relatively inexperienced members on the P³LA in a conservative, iterative, step-by-step fashion. As a necessary result most of the practical network planning was on a short-term basis, without adequate consideration given to long-term problems and solutions.

B. PROBLEM STATEMENT

The fundamental problem examined here extends out to the current planning horizon: what is required for Monterey BayNet to be a viable, self-sustaining and reliable community network for K-12 schools?

This central question invokes a host of others. First and foremost is the sustainability question of ownership: who owns the Monterey BayNet? When there are a myriad of different subscribers, many possibilities exist for their coordination.

One of the members (or a single joint agency) can act in behalf of all, limited voluntary coordination can occur, or subscribers can act individually with minimal coordination. In any case the principle of "residual claimancy" holds true as in any ownership: the owner assumes the risks of the decisions, and in return can claim the consequences or "residuals," good or bad, for that decision (Heyne 94).

A second sustainability question is as important as the first: what is the long-term mission of the network? Trying to sustain a network without understanding its mission is equivalent to searching for a solution without knowing the problem. Once the mission is clearly identified and stated, decisions can be made and evaluated against that mission. Until recently, most decisions for the network have been made with technical connectivity as the focus, not manageability and sustainability (Bigelow 95).

How will the network be maintained or managed? As stated in Chapter I, networks of any significance needs to be managed. What is network management and how does it relate to the sustainability of Monterey BayNet? What are the alternatives?

Networks require investment of capital and maintenance costs to sustain their operations. A summary of these costs follows (although not all apply to every site):

- (1) Router
- (2) Tranceivers
- (3) CSU/DSU
- (4) Modems (some sites that provide dial-in service)
- (5) Medium (Cable - 10Base5, 10Base2, 10BaseT, etc.)

- (6) Workstations (existing units integrated into the network as much as possible, may require purchase of network adapters or interface cards) (CDE 1994)
- (7) LAN wiring and installation charges (typically 20%-40% of individual network hookup costs) (CDE 1994)
- (8) Software
- (9) Frame Relay service charges (PacBell)
- (10) Network service charges
- (11) Internet service provider (ISP) charges
- (12) Training

Some of the allocation for costs above are well established. For example, the schools and organizations (subscribers) pay for their own routers, CSU/DSUs, wiring, LANS, software and connection provider charges.

Other charges are "shared" such as Internet service provider (ISP) and network management (NOC/NIC) charges. How will these costs be allocated? A line must be drawn across the network topology to clearly delineate who will pay for what. That line will be somewhere between a centralized single source and keeping the costs closer to the users at the sites. How will the fiscal accounting be handled and by whom? How will network service charges be recorded and collected?

There is also the sustainability question of standards. There exist published standards by CCITT, ISO, and IETF, and there are *de facto* standards dictated by current practices in the marketplace. Interoperability is enforced by prudent selection and uniform application of standards. In an area where functionality is so closely linked to interoperability, who will provide strong and competent decision-making on

standards important to the sustainability of Monterey BayNet? Are there any recommended standards?

Last are the questions regarding network management systems and operations. Which network management systems are the most cost effective? Which have the best potential performance for Monterey BayNet? How shall the Network Operations Center (NOC) and Network Information Center (NIC) be staffed? What services will be offered?

Answers to some of these questions may become apparent as issues are explored and a corresponding understanding is gained regarding network management.

C. SUMMARY

The many dimensions of the problem statement are enumerated by the list of questions in Figure 3.1. Viability, sustainability, and reliability are the critical qualities needed which lead to all other aspects of the K-12 network management problem.

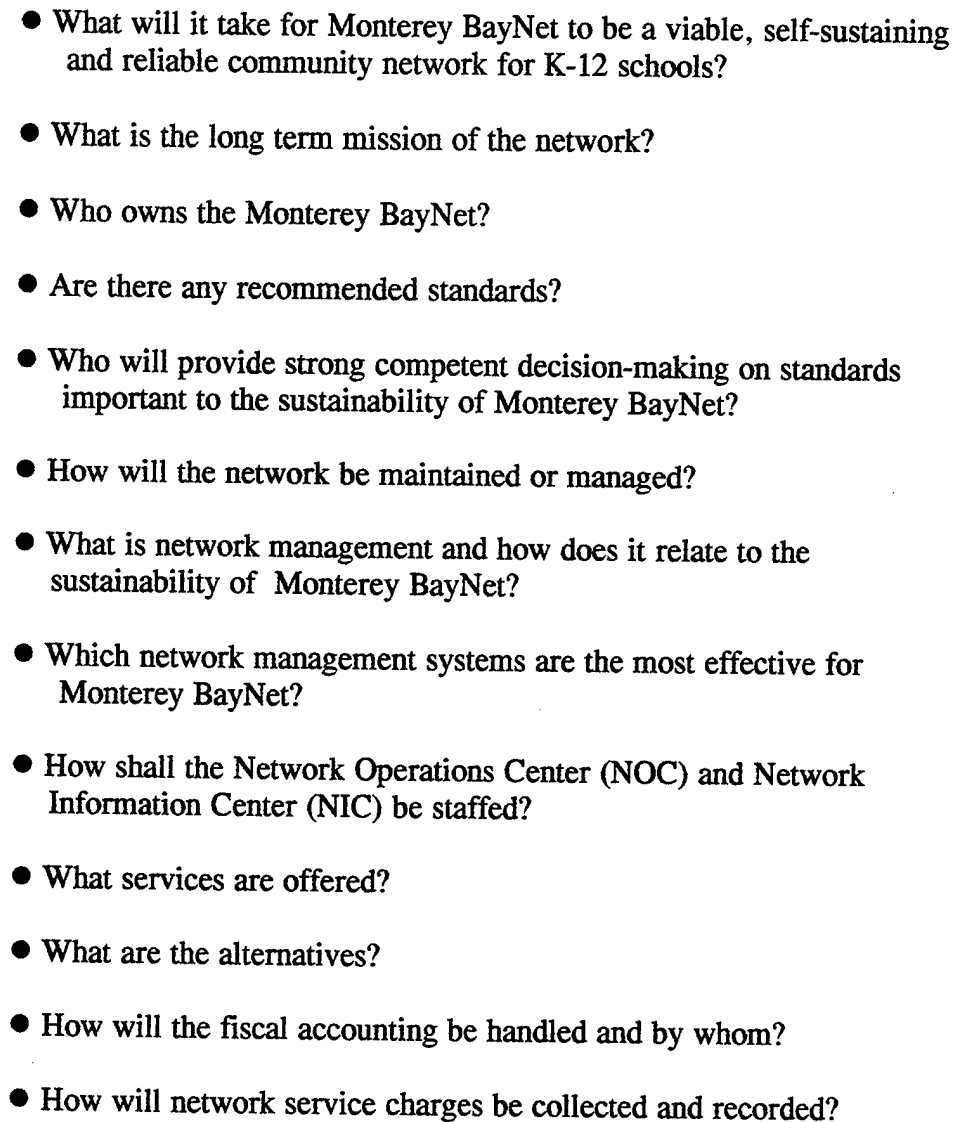
- 
- What will it take for Monterey BayNet to be a viable, self-sustaining and reliable community network for K-12 schools?
 - What is the long term mission of the network?
 - Who owns the Monterey BayNet?
 - Are there any recommended standards?
 - Who will provide strong competent decision-making on standards important to the sustainability of Monterey BayNet?
 - How will the network be maintained or managed?
 - What is network management and how does it relate to the sustainability of Monterey BayNet?
 - Which network management systems are the most effective for Monterey BayNet?
 - How shall the Network Operations Center (NOC) and Network Information Center (NIC) be staffed?
 - What services are offered?
 - What are the alternatives?
 - How will the fiscal accounting be handled and by whom?
 - How will network service charges be collected and recorded?

Figure 3.1 Problem Statement, Present and Future Research Questions.

IV. NETWORK MANAGEMENT MODELS

A. INTRODUCTION

It is important to gain an overall understanding of network management, before getting to the details of day-to-day network management and how they affect the sustainability of Monterey BayNet. Models are formulated to gain a better understanding of network management and to optimize a network management structure. Ultimately the optimum network management model depends on tasks required to monitor and control a network, which in turn depend on the requirements of subscribers and users.

B. USER REQUIREMENTS

To efficiently and economically meet the demands placed upon a shared network, the network must be managed. As previously stated, "network management" often means different things to various individuals and organizations. "Responsibilities of Host and Network Managers - a Summary of Oral Tradition on the Internet" (RFC 1173) discusses some of these responsibilities, emphasizing the importance of responsible behavior from users, host administrators, and network managers to the continued cooperative nature of the Internet. Figure 4.1 is a list of requirements (or demands) placed upon network management (Lo 91) that has been adapted to apply to the particular needs of Monterey BayNet.

- Meeting the information needs of students, teachers, educators, administrators, and researchers in Monterey and Santa Cruz Counties in terms of availability, performance and stability.
- Meeting educational business needs of K-12 schools in Monterey BayNet.
- The ability to manage Monterey BayNet from a single location.
- The ability to control Monterey BayNet and its components.
- The ability to detect faults in Monterey BayNet proactively.
- The ability to effectively isolate and correct faults in Monterey BayNet.
- The ability to sense and monitor the performance of Monterey BayNet, allowing for the early detection and correction of problems while they are small and before they affect subscribing schools and organizations.
- The ability to support security enhancements to Monterey BayNet.
- The ability to support accounting and some system of business chargebacks for the sustained financial support of Monterey BayNet.
- The ability to facilitate long-term strategic capacity planning for Monterey BayNet on a network wide scale.

Figure 4.1 Network management requirements for Monterey BayNet.

Each of the requirements in Figure 4.1 are broad and sweeping in scope. They focus on descriptions, methods, and the standards of quality (the "how") to which network activities will be accomplished. This may be contrasted with the elements of *The Agenda for Education in California* (Eastin 95) in chapter 1, Figure 1.2, which define the purpose or ultimate goal (the "what") of network activities in light of the overall education mission.

C. MODELS

Many models have been developed in an attempt to organize and clarify network management systems and requirements. Each appears to accurately model an aspect of network management from a unique, clearly defined perspective. A consideration of each type of model yields more understanding of network management than a consideration of any single model. Three of the most common models are considered here: the Structural Model of network management, the System Life-Cycle Model of network management and the Open System Interconnection (OSI) Functional Model of network management.

1. Structural Model

The Structural Model of network management is also called "Conformant Network Architecture Management" model (Walles 93 and Milham 92). It portrays network management from the viewpoint segregating all management tasks or functionalities at five different layers of responsibility as shown in Figure 4.2.

STRUCTURAL MODEL

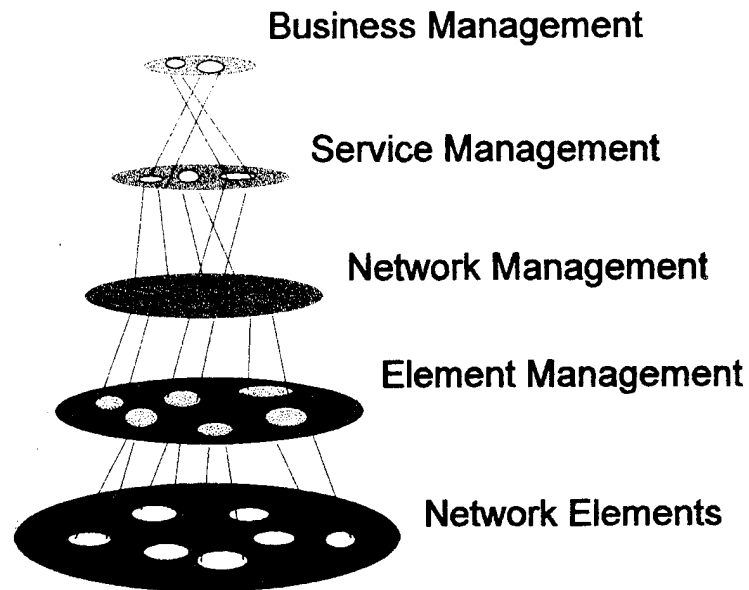


Figure 4.2 Structural model of network management (Walles 93).

The *Business Management Layer* of network management is responsible for enterprise-wide formulation of policies and strategies for the long-term sustainability and survival of the network. Tasks at this level of responsibility are regulatory and commercial in nature. When applied to Monterey BayNet as shown in Figure 4.3, the county Superintendents of Education (or designated representatives) might perform these tasks.

MODIFIED STRUCTURAL MODEL

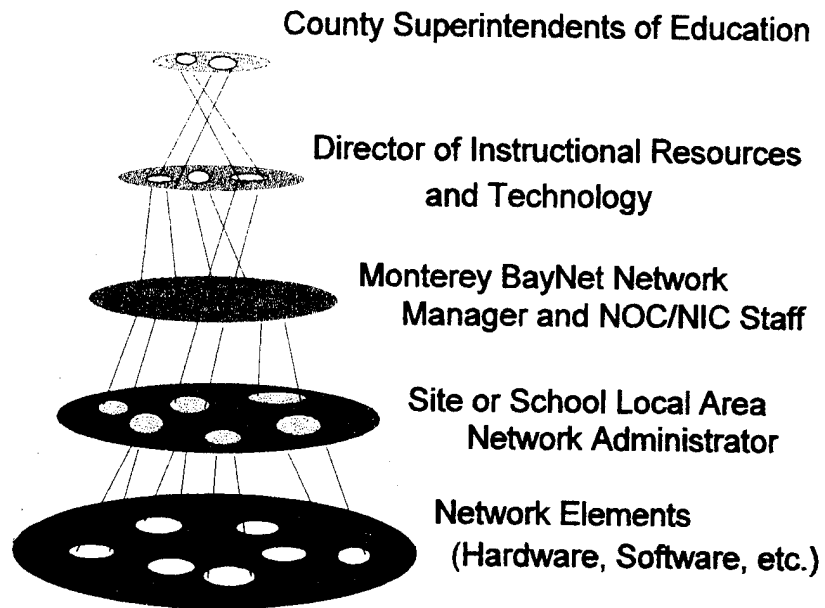


Figure 4.3 Modified Structural model of network management applied to Monterey BayNet.

The *Service Management Layer* of network management is concerned directly with customer (school and other network subscribers) interests. Tasks at this level implement the policies and regulations of the business layer in meeting the requirements of the customers. When applied to Monterey BayNet as shown in Figure 4.3, each county's Director of Education and Technology might perform these tasks.

The *Network Management Layer* is concerned with topological and connectivity aspects of the network (WAN components, network management software and hardware, routers and router software, domain nameservers and other Monterey BayNet shared services). Tasks at this level incorporate proficiency with the detailed operation of all technical aspects of the network as well as the more strategic issues addressed by the layers above. When applied to Monterey BayNet as shown in Figure 4.3, the Monterey BayNet network manager and the Network Operation Center (NOC)/ Network Information Center (NIC) staff might perform these tasks.

The *Element Management Layer* of network management is concerned with managing the network infrastructure at the school and other sites (LAN components, servers, hubs, workstations etc.). Tasks at this level involve direct contact with equipment for optimization of network performance. Direct contact with students and other users is also needed for optimization of requirements. Site or school LAN administrators, high school student volunteers, or supervised community volunteers might perform these tasks.

The *Network Element Layer* of network management is concerned with the functions of the actual elements themselves in the support the network. This includes application software, LAN software and hardware, workstations, printers etc. As one moves down the cone, responsibility and tasks are more widely distributed among an increasing number of entities.

2. System Life Cycle Model

The System Life Cycle Model of network management (Figure 4.4) portrays network management from a chronological and evolutionary viewpoint. The life of a network is broken into three distinct phases: Pre-Service, In-Service, and Future Service (Walles 93).

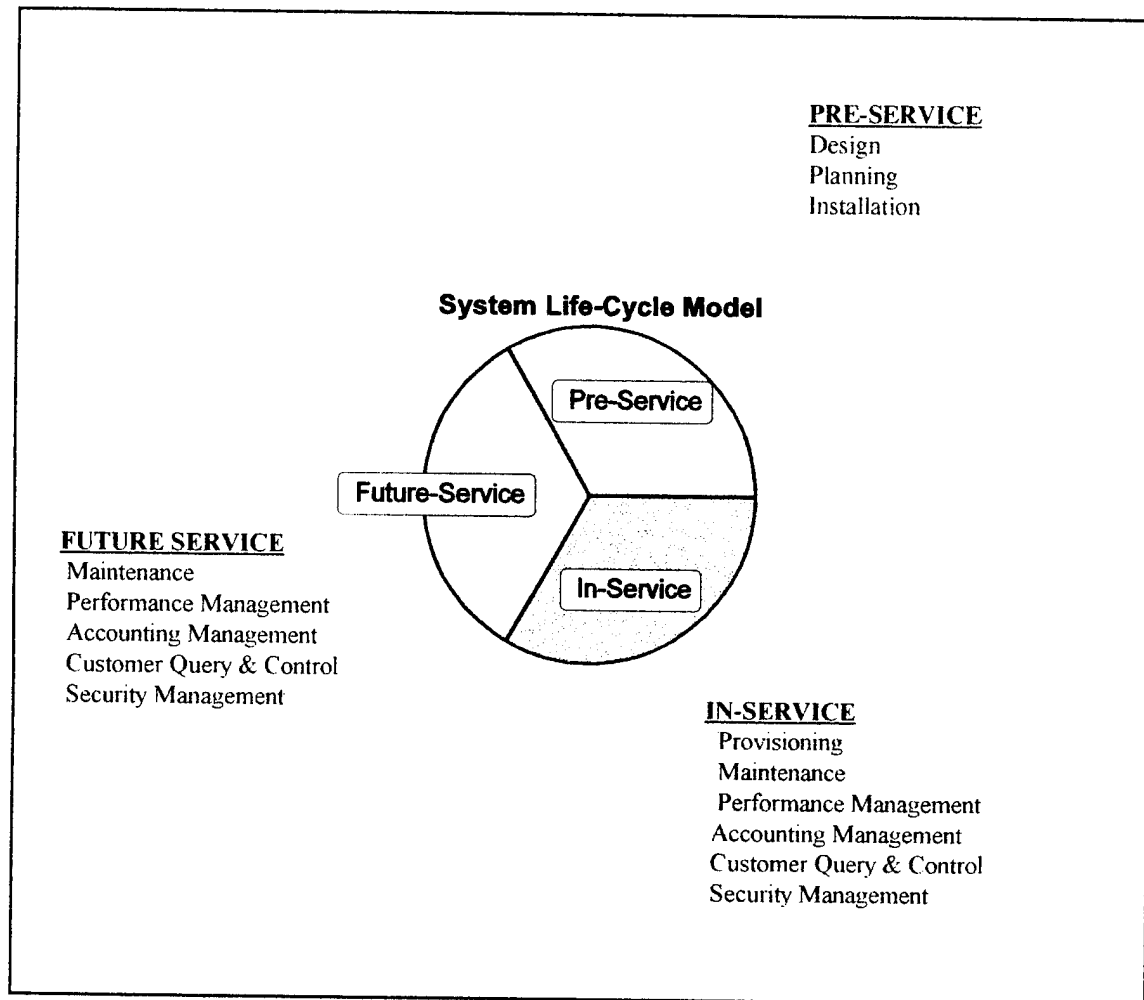


Figure 4.4 System Life Cycle model of network management (Walles 93).

This model identifies nine distinct functional tasks (Figure 4.5) assigned to the parts of the telecommunication network life cycle for which they are applicable (Walles 93).

- Design: engineering and documentation of network components, customer (site or school) premises equipment (CPE), and service provider (carrier or Internet) equipment based on the requirements of the network.
- Planning: business layer (county superintendent of education) decisions to introduce services in a cost effective manner while still keeping all of the requirements.
- Installation: the proper placement of network elements.
- Provisioning: activating network resources to meet the requirements of the customer (sites and schools).
- Maintenance: surveillance, preventative measures, and corrective measures performed during the life of the network.
- Performance Management: maintaining quality service for optimum network operation.
- Accounting Management: cost allocation, billing, and payment methods.
- Customer Query and Control: allow educators access to areas of network management functionality, inquiries about accounting.
- Security Management: measures to provide:
 - Authentication: transmission of criteria that validate the identity of the sender.
 - Non-repudiation: proof of origin of a transmission.
 - Integrity: criteria that prove to the recipient the data has not been modified.
 - Confidentiality: confidence that the transmission has not been intercepted.

Figure 4.5 Functional tasks of the System Life-Cycle model (Walles 93).

3. Open System Interconnection (OSI) Functional Model

The OSI Functional network management model (Figure 4.6) is probably the most widely known (Stallings 93). It breaks network management into five distinct functional

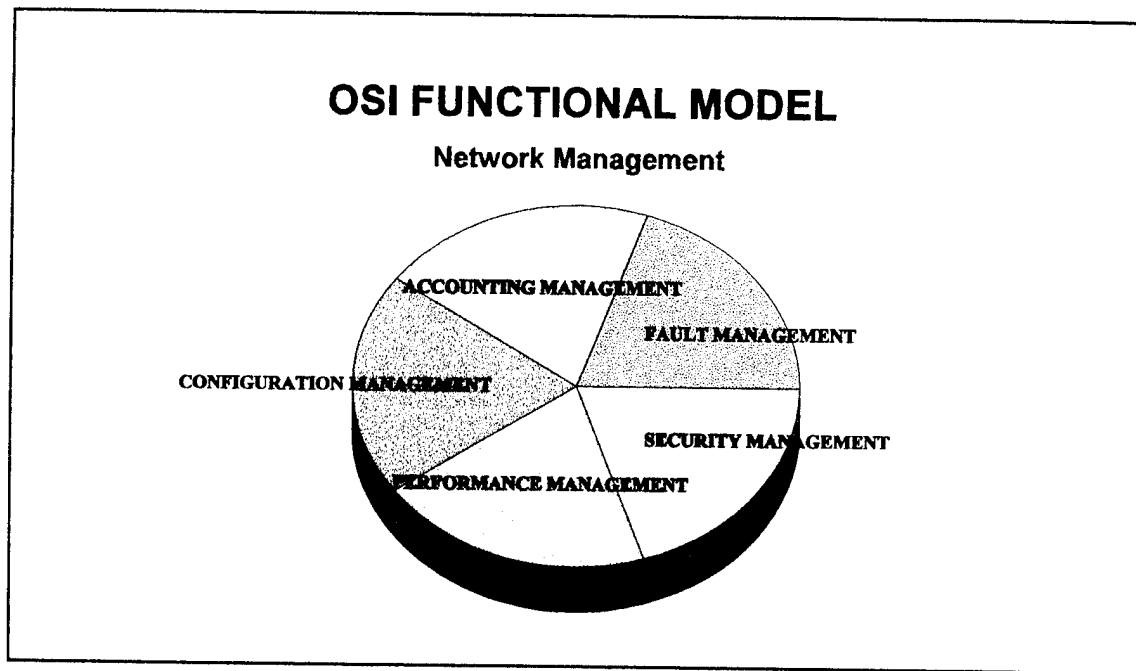


Figure 4.6 OSI Management functional model of network management (Stallings 93)

areas. These areas are fault management, accounting management, configuration and name management, performance management, and security management. Although each of the other models portray a unique perspective and contribute to a global understanding of the network management task, the OSI model is the simplest and most all-encompassing. Each functional management area contributes to the operation of the network (Stallings 93)(Sugarbroad 90). Network management tasks described here are properly the responsibility of the network manager and network operations staff.

a. Fault Management

Fault management tasks ensure that the network as a whole, and each component individually operate properly. When a failure occurs, action is taken to:

- find the fault.
- isolate the effects of the fault.
- reconfigure the network to minimize the effects of the fault.
- replace or repair the faulty component.
- restore the network to optimal configuration.

b. Accounting Management

The essence of telecommunication networks is the sharing of information systems and resources among many dispersed users. Procedures are often instituted to facilitate the sharing of costs incurred and services provided by the network. The network manager might account for use of network resources for reasons including:

- prevent any segment of users from abusing network resources at the expense of other users.
- facilitate procedural revisions for optimum network performance.
- conduct trend analysis for future growth projections.
- generate an equitable and reliable chargeback process.

It must also be noted that the costs of accounting management may be excessive if conducted on a per-year basis or per-site basis. Often accounting management goals can be achieved without establishing elaborate procedures.

c. Configuration and Name Management

Networks have incredibly sophisticated hardware and software components. Engineered to allow the maximum flexibility in network design, these components can be physically connected and internally configured in a seemingly infinite number of ways. Additionally, configuration updates can be performed on components to accomodate changes in network growth, topology, or usage patterns.

Because the network shares its resources among its own users and the rest of the world, there must be a way to identify and specify each component for access by users. Standard naming conventions are established to allow components to be identified uniquely. Name management is the method by which standard naming conventions are applied to designate network components.

d. Performance Management

Performance management can be divided into two areas: monitoring and control. Monitoring the network consists of continuous sensing and observing of network parameters. Control allows adjustments to be made to these parameters to keep them within optimum performance limits. The performance of the network is often a critical factor in the proper operation of certain applications. Network performance parameters are adjusted to control capacity, prevent bottlenecks, increase throughput, and decrease response time.

e. Security Management

Network security is concerned with maintaining the integrity of the information on the network itself. It includes, but is not limited to:

- Generation and dissemination of user accounts and passwords.
- Handling encryption keys.
- Firewall server configuration and operation, i.e. limiting the number of services available to users in an attempt to reduce network security vulnerabilities.
- Personnel access control of all network nodes.

D. SUMMARY

Network management models are different ways to break down the complex task of managing networks into smaller, more easily understood pieces. The OSI Functional Model will be used in later chapters to amplify network management and the role it plays in sustainability of Monterey BayNet. Irrespective of the model used, the network management task is driven by user requirements.

Even though occasional outages may occur, users require fast and reliable resolution of problems. This requirement requires rapid fault-detection and diagnostic fault management in the network. "Client Requirements for Real-Time Communication Services" (RFC 1193) provides more guidance on user requirements.

Charging algorithms and reports may be generated in the managing of accounts of the network because users expect operating costs to be distributed fairly. Care must be taken to prevent charging mechanisms themselves from imposing unfair costs. The configuration and domain names of the network are managed because users expect to

name network resources to access and employ them. The performance of the network is monitored and controlled because users require the network to deliver consistent, reliable service to support their applications. Finally, the security of the network is managed to protect network material and information resources and make them available only to authorized users.

V. CAPACITY AND RELIABILITY PLANNING

A. INTRODUCTION

The network management process actually began during the design planning of Monterey BayNet. According to the System Life-Cycle model depicted in Figures 4.4 and 4.5, network management also involves "preservice activities" of design, planning, and installation (Walles 93). Because some preservice decisions involve long-term commitments, it is important to consider network management when making some decisions that have an important role in charting the future direction of the network. Among the most important of these design decisions are capacity and reliability.

B. CAPACITY PLANNING

Capacity refers to the ability of a network to carry digital signals and is related to the maximum data rate that a network can carry (Stallings 94). The theoretical maximum capacity of any medium depends directly on the maximum frequency range or *bandwidth* of the medium. *Capacity Planning* is a concept that focuses on future requirements. It ensures that "adequate resources will be available to meet the future demands in a cost-effective manner while meeting the performance objectives." (Lynch, Rose 93)

Immediately after the benefits of a wide-area network (WAN) for the educational and research community were identified, capacity requirements for Monterey BayNet were identified and discussed. The "I³LA Network Design Tiger Team White Paper" (Brutzman 94) presents the purpose of Monterey BayNet, discussing performance

requirements and technologies available as a function of the types of organizations involved. To simplify and standardize the performance categories of these organizations, the network was divided into tiers (Figure 1.3). The importance of capacity considerations when on planning the network cannot be overemphasized. Like a stack of cascading dominoes, it affects most future decisions in some way (Figure 5.1).

- Type of Medium
 - Twisted pair
 - Coaxial cable
 - Optical fiber
- Network Access Standard (X.21 circuit switched, X.25 packet switched, ATM, Frame Relay, ISDN, etc.).
- Network (end to end) Protocol
- Routing (between routers) Protocol
- Number of independent network channels (e.g., administrative network, student network)
- Type of Pacific Bell network service and capacity available :

| | |
|---------------|------------------------|
| - ISDN | 64 Kbps - 1.544 Mbps |
| - SMDS | 1.544 Mbps - 34 Mbps |
| - Frame Relay | 56/64 Kbps - 1.54 Kbps |
| - ATM | 45 Mbps, 155 Mbps |
- Network Topology (Linked physical and logical configuration, i.e. a map of the network)

Figure 5.1 Decisions affected by capacity planning (Stallings 93)(Pacific Bell 95)

To insure interoperability of Monterey BayNet network components, these areas were explored in detail and decisions were agreed upon before purchasing routers, CSU/DSUs and other network components and services (Bigelow 95).

It is not only important to consider how capacity affects future decisions, but also how constraints are associated with that capacity. Capacity constraints include medium or circuit speed, protocol processing speed, and speed of the packet switches (Lynch, Rose 93). Additional consideration of these limitations may affect the choice of media, protocol, and type of network communication service.

After limitations of the chosen capacity are identified, methods of optimizing the selected capacity called *capacity relief* methods can be explored and factored into the design of the network topology. Some methods for capacity relief are displayed in Figure 5.2.

- increase link bandwidth by topology changes
- parallel circuits with load sharing
- private transmission facilities (wireless)
- Inverse multiplexing

Figure 5.2 Capacity relief methods (Stallings 93).

Redundancy in capacity and reliability is provided by alternate paths through the County Offices of Education to the High Schools. Provision for an additional future administrative network capability in Monterey BayNet increases the total capacity by

providing parallel circuitry. The use of wireless T1 capacity was discussed to provide Internet service connection between the Monterey and Santa Cruz county sections of the network, but two independent network connections from California State University Network (CSUnet), one to each county section of the network, were chosen instead. This choice was cost effective, more redundant for enhanced reliability.

More importantly, these choices were in compliance with current inter-LATA regulatory restrictions. Normally, current federal regulations only permit long distance carriers (e.g. AT&T, MCI, SPRINT) telecommunication access between telecommunication districts called Local Access and Transport Areas (LATAs). The Monterey county portion of the network is in LATA 8 and the Santa Cruz county portion of the network is in LATA 1. Instead of a single Internet service connection for all of Monterey BayNet, each LATA has its own Internet Service connection. This eliminates the need for long distance carrier service to communicate Internet service between LATA 1 and LATA 8.

C. RELIABILITY

Reliability refers to the sustainability of network operations over the short term. Network managers have several different measures for reliability as shown in Figure 5.3.

These items when considered together form an important indication to the network manager regarding how well the network is performing. The first two items in Figure 5.3 are almost self-explanatory. *MBTF* answers the question of "how often and how hard it breaks." *MTTR* indicates "how effectively we can fix it." *Availability*

- Mean time between failures (MTBF)
- Mean time to repair (MTTR)
- Availability (Percent Up-time = $[\text{Total Time} - \text{Down Time}] / \text{Total Time}$)
- Response times

Figure 5.3 Measures of reliability (Lynch, Rose 93).

indicates the performance of the network in terms of the percentage of time that the network is available as a service to all subscribers. *Response time* is an indication of how well (or how poorly) the network is performing its service. It is experienced by the user as the speed or sluggishness with which an application running across the network performs. These concepts will be discussed further in Chapter VI and are important concepts when running a network operating center (NOC).

Methods to increase network reliability are listed in Figure 5.4.

- redundant regional backbones
- multiple connections to backbone suppliers
- fail-over back-up routing
- robust topologies with path separation between connections
- stock of ready spares

Figure 5.4 Methods to increase network reliability(Lynch, Rose 93).

Reliability in Monterey BayNet is provided by (1) multiple connections to service provider (CSUnet), i.e. one for the Monterey county portion of the network and

one for the Santa Cruz portion, (2) back-up routing of the Internet to K-12 schools from the service provider through the T1 connection to the County offices of Education, and (3) a robust network topology with separation of connections in the provision of physically separate administrative and student networks.

D. SUMMARY

Capacity and reliability are fundamentally important in the operational planning of a network because together they contribute to the functionality and performance of the network. Performance is central to the long term sustainability of Monterey BayNet because it involves meeting educator, researcher and user requirements for an information resource they can depend on consistently for their information needs.

Sustainability is an economic issue as well as a performance issue. Capacity and reliability have costs, and it is important to balance performance needs against costs. Costs of connectivity to the Internet (CSUnet), of site connectivity and redundant links (Pac Bell), of network management, and costs of ready spares must be balanced against the benefits of the network and available funding. The value of network and Internet information resources must be assessed against the costs so that the point of diminishing marginal returns is not exceeded (Emery 87). Network management functions optimize performance and minimize costs to increase sustainability of Monterey BayNet.

VI. NETWORK OPERATING CENTER (NOC) FUNCTIONS

A. INTRODUCTION

"A well-functioning Network Operations Center (NOC) is critical to the successful operation of a network" (Lynch, Rose 93). Network operations ensure that the hardware and software components of a network run efficiently and effectively (California Department of Education 94). This is critical to the success of the education mission of the Monterey BayNet. The use of interactive multimedia in many classrooms will produce large and rapidly varying data rates, thus requiring adequate bandwidth. The NOC is the location of a network management station and personnel who run the network. This may be a single, remotely monitored microcomputer workstation for smaller networks. Larger networks typically have network management workstations on the desks of the manager of the facility, network programmers, network operators, and at the help desk.

A collection of documents called "Request for Comments (RFCs)" constitute a useful body of historical, technical, informative and administrative knowledge concerning the evolution and operation of the Internet, and the day-to-day operation of the NOC. Originally, they grew informally. Some evolved into Internet standards, others remain "For Your Information" (FYI). The collection is extensive (presently there are more than 1700) and continues to grow. RFCs are numbered in chronological order. The scope of topic matter is also extensive. RFCs are among the many important tools for the proper managing of networks and will be referred to frequently.

Network management software is also essential in the operation of the NOC.

"FYI on a Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices" (RFC 1147) provides a 126 page tutorial on network management and a catalog of network management tools. Tools specific to the network management functional areas will be discussed with each area.

B. FAULT MANAGEMENT

The goals of fault management can be enumerated in order of priority as follows (Aidarous, Plevyak 94):

- to restore service in the presence of faults.
- to discover the root cause (the smallest repairable unit that contains the fault).
- timely and efficient repair of the fault, conserving labor and material costs.
- to collect and analyze information on the cost of service interruption and cost of repair, so that a good balance of resources can be allocated to achieve a balance between service and costs.

Figure 6.1 Goals of network fault management (Aidarous, Plevyak 94).

1. Network Monitoring Display

Most network management software programs have Graphical User Interfaces (GUI) to display network management in a variety of user-friendly and informative views. Network maps can be presented geographically (Figure 6.2), topologically (Figure 6.3), in a partitioned view (Figure 6.4), or with individual hardware component

indications (Figure 6.5). Major design criteria of such displays includes the rapid and efficient identification, isolation, and repair of network faults. In addition to automatic updates and intuitive display features, certain network management software programs permit query of network components and functions for more information. These features combine to make modern network management systems proactive in optimizing network performance, and reactive in signaling network failures that require immediate operator action to prevent a system-wide failure.

Geographic displays (Figure 6.2) place emphasis on the relative physical location of components and long-distance links, as well as the types of connections and nodes. Topological displays (Figure 6.3) emphasize network management on a site level and are more functional than positional. These usually include routing equipment and communications media. The partitioned view (Figure 6.4) of a network further decomposes the network to "end-systems equipment" (workstations, servers, printers etc.) with a focus on individual equipment links. The component level (Figure 6.5) stresses the status of individual equipment hardware or software. It can be in graphical or tabular form.

Some displays start with a very high, abstract level (one icon at the root level to represent the entire network), and consecutive clicks on the icons decompose the display into successively more levels of detail, until the bottom component is reached. Many variations are possible and can often be configured directly by the end user.

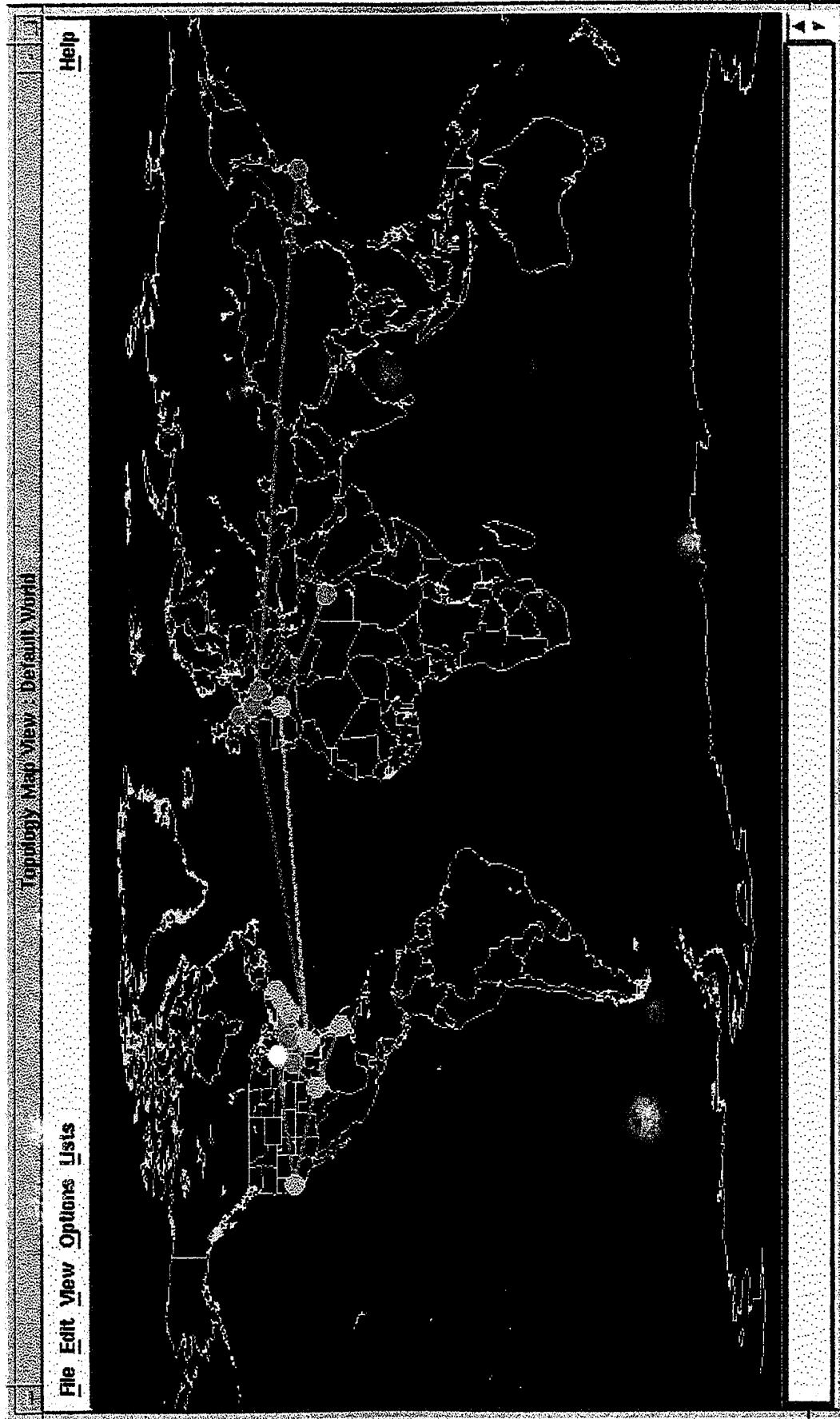


Figure 6.2 Geographic Network Map ©1995 Racal-Datcom



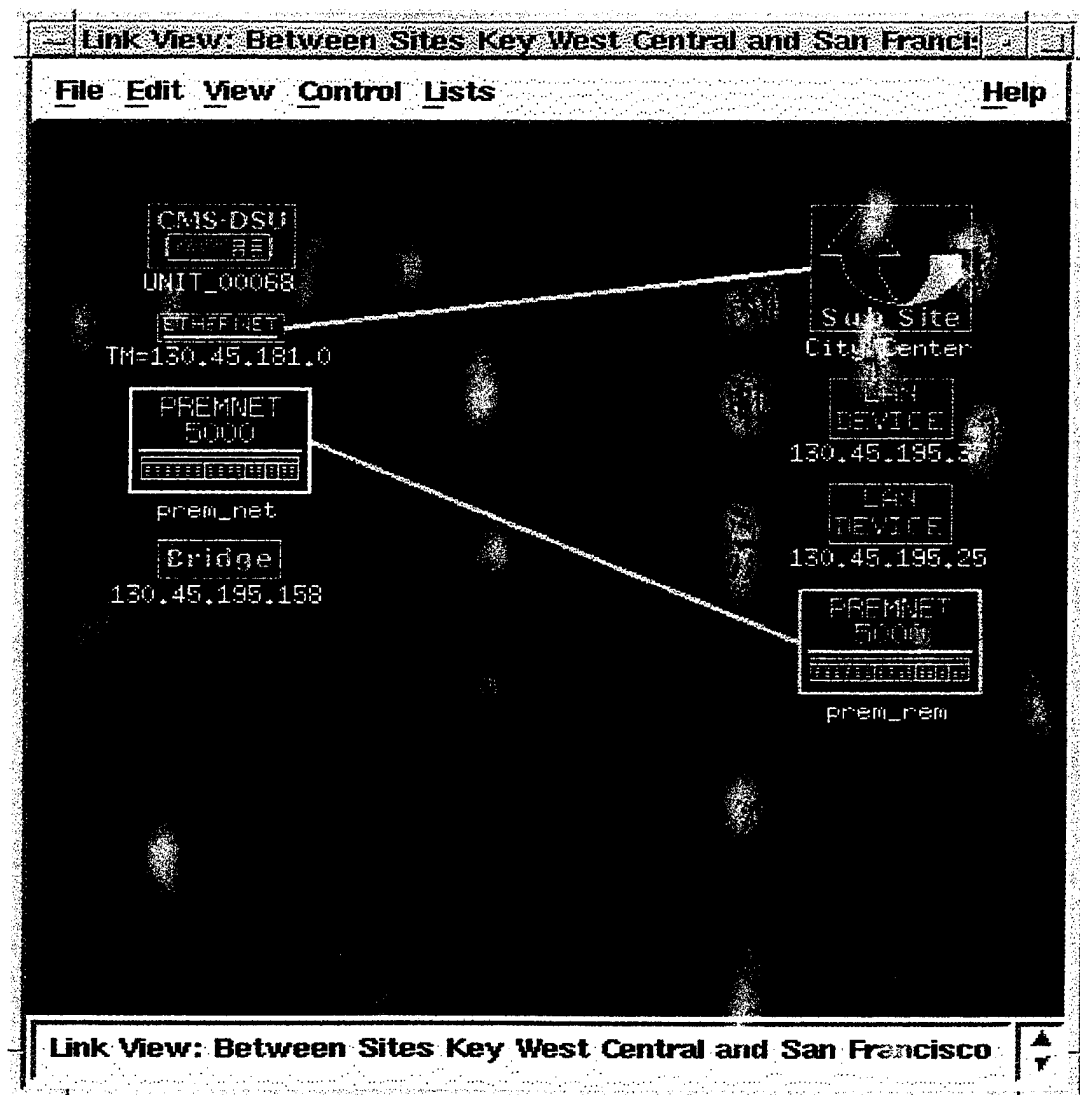


Figure 6.4 Network Link View Map ©1995 Racal-Datacom

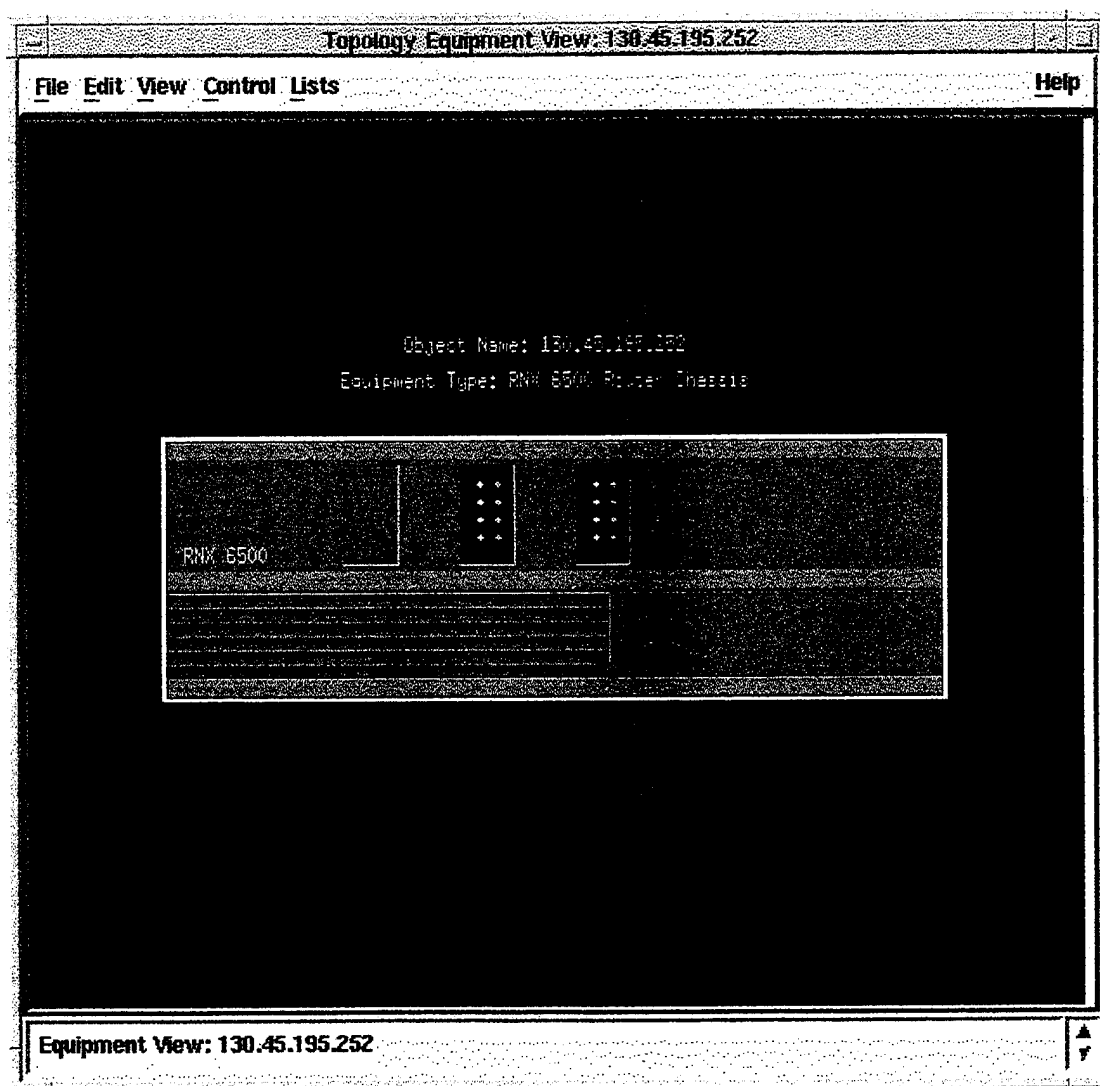


Figure 6.5 Equipment View ©1995 Racal-Datacom

Some network management software has color coded component icons and links in displays to indicate the state of the network dynamically (Table 6.1). On some applications, normal operating link color can vary on a continuous color scale with higher traffic flow as shown in Table 6.1. In addition, links and icons can be selected with a mouse to open another window that can display the attributes of the selected component.

| ICON COLOR | LINK COLOR | STATUS | MEANING |
|------------|-------------|----------|------------------|
| BLUE | BLACK | Unknown | Indeterminate |
| | BLUE-PURPLE | Normal | Normal Operation |
| YELLOW | YELLOW | Marginal | Object Impaired |
| RED | RED | Critical | Non Functional |

Table 6.1 Icon and link dynamic display color scheme (IBM 93).

2. Network Faults, Fault Identification and Isolation

There are basically two categories of network faults (IBM 93):

- Device Errors - hardware or software failures at a specific node.
- Connectivity Errors - lack of communication between nodes, usually attributable to a subtle device error.

Figure 6.6 Categories of network faults (IBM 93).

Most device errors, or ("hard" failures) are indicated clearly and unambiguously on the network management station displays at the time of their occurrence. Location and

isolation is often possible using the network management station.

Connectivity errors are more difficult to diagnose, often involving degradation of performance or faults of an intermittent nature. Symptoms of connectivity errors include:

- Previous ability to reach a node followed by no access
- Error that indicates connection timed-out:
 - remote end system down
 - routing problem
 - the default gateway has a problem
 - poor network throughput (low data flow rate)
- User received an error that a remote system could not be found:
 - remote system was powered off
 - a component was removed
 - hostname-to-IP map *ping* problem
 - gateway does not have remote system in its routing tables

Figure 6.7 Symptoms of connectivity errors (IBM 93).

To test whether a connectivity problem is the cause for the degraded condition, the following actions can be taken at the network management station (IBM 93):

1. Select a polling test at the IP, TCP, and SNMP layers and ascertain whether the remote site is connected to the management station.
2. Conduct a *ping* test to verify connectivity at the IP layer and determine the number (or percentage) of packets sent that were lost.
3. Locate Alternate Route Between Nodes to circumvent traffic around the problem area.
4. Gather connectivity information to the remote node:
 - gateway routing tables for the remote node.
 - address translation tables for the remote node.
 - determine IP and link addresses for the remote SNMP node.
 - determine network services available on the remote node.
 - use *ping* to determine the route between remote node.

3. Alarm Generation and Threshold Definition

Before alarm generation can be addressed, the concept of "events" (or SNMP traps) must be introduced. Events are generated by all agents (remote nodes on the network in communication with the network management station) when certain conditions occur at that agent. Examples of this include:

- a preset threshold limit was exceeded
- network topology changed (components added or deleted)
- an error occurred (inconsistent or unexpected behavior)
- an object (router, workstation, printer, server etc.) or interface (port) changes status to up or down in response to a *ping*
- node configuration changes
- an SNMP trap received from a managed node

Figure 6.8 Examples of Network Agent Events (IBM 93).

Events are categorized and numbered according to a standardized numbering scheme and logged automatically in an event log file. Table 6.2 shows an example list of numbered events (IBM NetView/6000 93). Additional information about the agent is provided by an SNMP trap. This additional information includes the agents' object (data field), IP address of that agent, event number, time stamp, name of the node, enterprise-specific variables and event description. Events can then be handled using an application that creates a dynamic events display. Figure 6.9 shows an example events

display. After an event is generated, displayed and logged as described above, it is placed into a historical file for subsequent trend analysis.

| NUMBER | EVENT |
|--------|------------------------|
| 0 | Cold Start |
| 1 | Warm Start |
| 2 | Link Down |
| 3 | Link Up |
| 4 | Authentication Failure |
| 5 | EGP Neighbor Loss |
| 6 | Enterprise Specific |

Table 6.2 Event number vs. event descriptions (IBM 93).

4. Alarm Processing

Alarms are generated when certain events occur or predefined operator performance limits are violated. The alarms may be audible, visual or some combination of both. An update of the display typically accompanies the alarming condition to assist in rapid identification of the failure.

5. Trouble Ticketing

When an incident is created by an event, by an alarm, or by the operator, a trouble ticket can be generated. A trouble ticket is a file and a hard copy form. As with the generation of many alarms, the generation of trouble tickets is a function of limits preset by the network operator. The trouble ticket is created to assist operators in

| File Edit Options | | Event Monitor | | Help |
|---|-------------------------------|---------------------|------------------|-------|
| <div style="display: flex; justify-content: space-between;"> <div> <input checked="" type="checkbox"/> All Objects <input checked="" type="checkbox"/> Selected Objects or AMMs <div style="border: 1px solid black; padding: 2px; width: 100px; margin-top: 5px;">Edit List</div> </div> <div> AMM Name(s) SNMP.01 <div style="display: flex; align-items: center; margin-top: 5px;"> <input type="checkbox"/> Base Objects Only </div> </div> </div> | | | | |
| <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div> Event Selection: <input checked="" type="checkbox"/> Alarms <input checked="" type="checkbox"/> Value Change </div> <div> <input type="checkbox"/> Canceled Alarms <input checked="" type="checkbox"/> Attribute Change </div> <div> <input checked="" type="checkbox"/> Enrolls <input checked="" type="checkbox"/> System </div> <div> <input checked="" type="checkbox"/> Deenrolls <input checked="" type="checkbox"/> Generic <input type="checkbox"/> Reenrolls </div> </div> | | | | |
| <div style="display: flex; justify-content: space-between; align-items: center;"> <input checked="" type="checkbox"/> Monitor Events <input checked="" type="checkbox"/> Historical Events <div> Time/Date : From 11/28/1994 00:00:00 to 11/28/1994 23:59:59 </div> <div> <div style="border: 1px solid black; padding: 2px;">Get Events</div> <div style="border: 1px solid black; padding: 2px;">Reset Criteria</div> </div> </div> | | | | |
| Filtering On All Objects, Selected Events, From 11/28/1994 00:00:00 to 11/28/1994 23:59:59 | | | | |
| Event # | Object Name | Received on | Event Type | Agent |
| 659 | Miami | 11/28/1994 13:57:47 | Attribute Change | T |
| 658 | Allow LAN Discover Broadcasts | 11/28/1994 13:57:05 | Attribute Change | T |
| 657 | John DOE | 11/28/1994 13:56:32 | Enroll | T |
| 656 | CMS400.01 | 11/28/1994 13:56:07 | Enroll | T |
| 655 | CMS400.01 | 11/28/1994 13:56:07 | Enroll | T |
| 654 | Event Days to Keep | 11/28/1994 13:55:31 | Attribute Change | T |
| 653 | Update SNMP Info Time | 11/28/1994 13:55:07 | Attribute Change | T |
| <div style="display: flex; justify-content: flex-end; gap: 10px;"> <div style="border: 1px solid black; padding: 2px;">Detail</div> <div style="border: 1px solid black; padding: 2px;">Clear List</div> <div style="border: 1px solid black; padding: 2px;">Add Object</div> </div> | | | | |
| Historical Events | | | | |

Figure 6.9 Events Display

tracking problems from onset through resolution. It also records fault indications and alarms. In some network management systems, e-mail notifications are automatically created and transmitted to various concerned individuals when the trouble ticket is issued, and automatic pager activation is also possible. Activities taken during problem resolution and those that actually solved the problem are recorded along with the rest of the data. This data can be used for trend analysis or as a troubleshooting reference if the same or similar failure occurs in the future. "NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist ('NOC TT Requirements')" (RFC 1297) presents a detailed description of an architecture for an integrated trouble ticket system.

6. Troubleshooting Tools

In addition to the automated tools offered to network operators by fault management software programs, there are some other tools that can give network operators additional capabilities in their troubleshooting efforts.

"FYI on a Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices" (RFC 1470) provides 192 pages of information on hundreds of different network troubleshooting software tools. For each item the catalog provides a standard description, listing name, keywords, abstract, mechanism, caveats, bugs, limitations, required hardware and software, and availability. There is also an exhaustive cross reference catalog of software tools sorted by keyword. "A Primer on Internet and TCP/IP Tools" (RFC

1739) is a 45-page introductory guide that covers TCP/IP based utilities and applications. It describes the software-based tool, its application and (in many cases), how it works. It also provides session examples of many utilities. "Echo Protocol" (RFC 862) gives additional information on the *ping* procedure.

Three of the most common tools are discussed below: *ping*, *traceroute*, and *nslookup*. All of them are present on Unix platforms. *ping* was included in the Microsoft Windows and Macintosh (MacTCP Watcher) software builds distributed to Monterey BayNet workstations (Bigelow 95).

In the late 1970s the only tool that was used for network "management" was called the Internet Control Message Protocol (ICMP). ICMP is an integral part of the IP (Internet Protocol). It provides a way to transfer control information and feedback about errors, abnormal conditions, and query results from remote routers and hosts to the source of a message datagram for remedial action (Stallings 93). From a fault management perspective, the most useful feature of ICMP is the "echo-reply" feature because it provides an indication that communication is possible across a connection. Another message pair is called "timestamp-reply" which can be used to measure the delays that a packet experiences across a network (Stallings 93). The most widely used of these procedures is the ICMP *ping* procedure (Packet Internet Groper - acronym courtesy Dr. David Mills).

ping performs many functions, such as verifying whether a network device or network can be reached, or verifying the operation of a particular device or observer. The usefulness of *ping* lies in the fact that it can be used to confirm the operational status of

any remote host or addressable network component. It is used to determine round-trip times from which traffic conditions, congestion, and bottlenecks can be inferred.

Figure 6.6 is an actual example illustration some of the ways that the *ping* procedure can be used. If *ping* [hostname] or *ping* [IP address] is the only command given, then the return is a simple statement whether or not the packet has returned (i.e. "host is alive").

Different *ping* options exist to include the number of ICMP Echo_Request datagrams sent, the number of Echo_Response datagrams received, and/or round trip times (ms). When the -S switch is used as shown in Figure 6.10 (switch options may vary), the *ping* will retransmit the specified packet size (default is 64 bytes) for a specified number of repetitions (e.g. 10). A summary block appears with information on number of IP datagrams sent, number received, percent packet loss (note the missing datagram sequence numbers 7 and 10), and round trip times (ms)- min/avg/max. The major limitation of *ping* is that it cannot be used to determine which component in a serial train is responsible for lack of *ping* return.

As its name implies, *traceroute* is a tool that is used to discover the actual route taken by packets from source to destination. It permits collection of information about intermediate nodes to the destination. *traceroute* is built upon the ICMP time-exceeded error (time-to-live or *tll*) reporting mechanism (Lynch 93). Sometimes *tll* is also known as the "hop count". With each node that a packet passes along the route, *tll* is decremented by 1. When a packet arrives at an intermediate router with a *tll* = 0, that router sends the packet back to the originating host with information on its identification and time. The *tll* field is then incremented at a value 1 higher by the originating host

ping from Naval Postgraduate School, Monterey, California to various world locations
(use IP address or domain name, comments in parenthesis):

```
<66 sagan(SunOS) /sagan_ul/dmtrepan> ping 131.120.50.1      (SUBNET ROUTER)
131.120.50.1 is alive
<67 sagan(SunOS) /sagan_ul/dmtrepan> ping 131.120.254.51  (BARRNET ROUTER LOCAL)
131.120.254.51 is alive
<68 sagan(SunOS) /sagan_ul/dmtrepan> ping 13              (BARRNET ROUTER STANFORD)
131.119.75.1 is alive
<69 sagan(SunOS) /sagan_ul/dmtrepan> ping nps.navy.mil      (DNS PRIMARY)
nps.navy.mil is alive
<70 sagan(SunOS) /sagan_ul/dmtrepan> ping nic.ddn.mil       (MILNET NIC)
nic.ddn.mil is alive
<71 sagan(SunOS) /sagan_ul/dmtrepan> ping rhi.hi.is         (ICELAND)
rhi.hi.is is alive
<72 sagan(SunOS) /sagan_ul/dmtrepan> ping u-tokyo.ac.jp     (JAPAN)
u-tokyo.ac.jp is alive
<73 sagan(SunOS) /sagan_ul/dmtrepan> ping relay.huji.ac.il   (ISRAEL)
relay.huji.ac.il is alive
<75 sagan(SunOS) /sagan_ul/dmtrepan> ping mcmvax.mcmurdo.gov (ANTARCTICA)
mcmvax.mcmurdo.gov is alive
<76 sagan(SunOS) /sagan_ul/dmtrepan>                        (UNIX Prompt Back)
```

Ping -S option from Naval Postgraduate School, Monterey, California
to the Monterey County Office of Education, 10 times in 1 second
intervals with 64 Byte datagrams:

```
<107 altair(SunOS) /sagan_ul/dmtrepan> ping -s mcoe.monterey.k12.ca.us 64 10 (ping -S Switch option)
ping mcoe.monterey.k12.ca.us: 64 data bytes
72 bytes from monterey.k12.ca.us (205.155.43.2): icmp_seq=0. time=80. ms
72 bytes from monterey.k12.ca.us (205.155.43.2): icmp_seq=1. time=73. ms
72 bytes from monterey.k12.ca.us (205.155.43.2): icmp_seq=2. time=80. ms
72 bytes from monterey.k12.ca.us (205.155.43.2): icmp_seq=3. time=76. ms
72 bytes from monterey.k12.ca.us (205.155.43.2): icmp_seq=4. time=78. ms
72 bytes from monterey.k12.ca.us (205.155.43.2): icmp_seq=5. time=74. ms
72 bytes from monterey.k12.ca.us (205.155.43.2): icmp_seq=6. time=76. ms
72 bytes from monterey.k12.ca.us (205.155.43.2): icmp_seq=8. time=72. ms

----mcoe.monterey.k12.ca.us ping Statistics----
10 packets transmitted, 8 packets received, 20% packet loss
round-trip (ms)  min/avg/max = 72/76/80

<108 altair(SunOS) /sagan_ul/dmtrepan>                        (Unix Prompt back)
```

Figure 6.10 *ping* features (comments in parenthesis).

and re-transmitted. By repeatedly incrementing the *ttl* field, subsequent nodes can be identified. The process is repeated until packets reach the final destination. As shown in figure 6.11, an actual *traceroute* was conducted between Naval Postgraduate School and the American base at McMurdo Bay, Antarctica. The screen shows name and IP address of each router along the path and round trip times to each node. If a *ping* failure occurs, the location of the failure is denoted by the !H symbol.

traceroute from Naval Postgraduate School, Monterey, CA to Antarctica:

<64 sagan(SunOS) /sagan_u1/dmtrepan> *traceroute* mcmvax.mcmurdo.gov

traceroute to mcmvax.mcmurdo.gov (157.132.103.50), 30 hops max, 40 byte packets

```
1  bargate.nps.navy.mil (131.120.254.51) 23 ms 3 ms 3 ms
2  Sd (131.119.75.1) 7 ms 7 ms 9 ms
3  Sd (192.31.48.200) 8 ms 13 ms 8 ms
4  ames.barrnet.net (131.119.2.10) 12 ms 10 ms 10 ms
5  ARC1.NSN.NASA.GOV (192.203.230.5) 14 ms 11 ms 10 ms
6  128.161.15.6 (128.161.15.6) 10 ms 10 ms 12 ms
7  MCMURDO.NSN.NASA.GOV (128.161.115.2) 595 ms * *
8  mcmurdo-gw.mcmurdo.gov (157.132.100.15) 597 ms 599 ms 591 ms
9  b165-net.mcmurdo.gov (157.132.107.11) 607 ms 592 ms 604 ms
10 mcmvax.mcmurdo.gov (157.132.103.50) 610 ms 594 ms 605 ms
```

<65 sagan(SunOS) /sagan_u1/dmtrepan>

Figure 6.11 *Traceroute* to Antarctica.

nslookup is a tool used to query nameservers concerning entries in the Domain Name System (DNS) database that pertains to a particular host or domain. (RFC 1739)

"A Primer on Internet and TCP/IP Tools" shows the most common use of *nslookup* is to determine host systems IP address from its name (Figure 6.12) or the hosts name from its IP address. The *nslookup* session can be non-interactive or interactive, and it displays a

unique prompt during the interactive session. *nslookup* has a set of preferences and modes called "option settings" that can be accessed using the "SET" command at the *nslookup* prompt (Albitz 93). EXIT is used to quit the *nslookup* application. In Figure 6.12, *nslookup* is typed without an argument, signalling the start of an interactive session. The name and IP address of the originating host are given and then a > prompt

Type *Nslookup* with no argument to enter the interactive mode:

```
<127 altair(SunOS) /sagan_u1/dmtrepan> nslookup      (Interactive mode is entered when no argument
is specified)
Default Server: nps.navy.mil
Address: 131.120.254.52

> mcoe.monterey.k12.ca.us                          (inserted DNS name at the prompt)
Server: nps.navy.mil
Address: 131.120.254.52

Non-authoritative answer:
Name:   mcoe.monterey.k12.ca.us
Address: 205.155.43.2                                (returned IP address)

> 192.203.230.5                                     (inserted IP address at the prompt)
Server: nps.navy.mil
Address: 131.120.254.52

Name:   ARC1.NSN.NASA.GOV                            (returned DNS name)
Address: 192.203.230.5

> 131.119.75.1                                       (inserted IP address at the prompt)
Server: nps.navy.mil
Address: 131.120.254.52

Name:   su-b.barnet.net                              (returned DNS name)
Address: 131.119.75.1

> exit                                               (exit from nslookup interactive session)
<128 altair(SunOS) /sagan_u1/dmtrepan>             (normal UNIX prompt back)
```

Figure 6.12 *nslookup* examples.

appears. When the domain name of the Monterey county office of education (mcoe.monterey.k12.ca.us) is entered, *nslookup* returns the address of the MCOE nameserver, 205.155.43.2 . An IP address is then entered, and the host name ARC1.NSN.NASA.GOV returned. Another IP address entered, and the hostname su-b.barrnet.net is returned. To exit the session, EXIT is typed.

C. NETWORK ACCOUNTING MANAGEMENT

Accounting management involves the ability to "answer for" the use of the network by individual schools and other sites. It involves systems that identify costs and enable charges to be established for the use of network resources. "Internet Accounting: Background" (RFC 1272) discusses alternatives in metering services and network usage reporting, and "Resource Allocation, Control, and Accounting for the Use of Network Resources" (RFC 1346) discusses network resource allocation, control and accounting.

1. Reasons for Network Accounting and Requirements

Figure 6.13 lists several reasons why it is important to account for the use of the network (Stallings 93). Because some of the information may ultimately involve the exchange of money, network accounting information is often protected from unauthorized access and tampering by the implementation of additional security features (firewalls, encryption, additional passwords, etc.).

- prevent one user or group from abusing access privileges and loading down the network at the expense of others
- assist users make more efficient use of the network
- provide data for future growth projections and planning
- provide accurate data on usage for billing purposes

Figure 6.13 Reasons for network accounting (Stallings 93).

RFC 1272 offers some additional motivations for usage reporting, listed in Figure 6.14.

- understand/influence behavior-feedback to subscribers on their own usage
- measure policy compliance of subscribers
- rational cost allocation and recovery

Figure 6.14 Additional reasons for network accounting (RFC 1272).

Network accounting also requires the establishment of a database. The minimum amount of information for this database (modified for Monterey BayNet application) includes :

- name of school or organization (subscriber)
- billing address
- location of equipment
- phone numbers of site representatives
- network address information
- credit account history
- type of link
- information about Customer Premises Equipment (CPE)
- service providing equipment
- billing information

Figure 6.15 Network accounting information (Aidarous 94).

To facilitate accounting, a network inventory must be maintained. Inventory management is required for account management because network resources must be known before usage of the resources is assessed. It involves a listing for location and identification numbers of network components such as hosts, routers, and bridges, the location of individual computers, networking software and site administrator (Lynch 93).

Some network management systems use an inventory database in conjunction with their fault management system or trouble ticketing system so that network resources can be readily identified when faults occur. This inventory database may be populated in a variety of ways. First and most obvious, the data can be inserted manually. For large networks, this job can be burdensome and time consuming. Some network management systems (e.g. AIX NetView/6000) have an "Automatic Network Discovery" feature.

When activated, the management station automatically polls the network from the management station outward, populating a network topology database with resource and configuration information as it comes back from the network agents. Special applications

allow the management program to map and communicate with nodes that use protocols other than SNMP/IP. This information is used to generate the graphical network display and can be exported for other uses, such as inventory management and accounting. IBM's AIX Trouble Ticket/6000 can import information from the network topology data base to populate its inventory database (IBM Trouble Ticket/6000 Users Guide 93), primarily for rapid fault isolation and then for inventory management.

2. Network Cost Sharing and Cost Accounting

Network accounting management also includes the subject of *cost sharing*. Before costs can be shared, they must be measured and accounted for. *Cost accounting* involves enumerating known costs for the purpose of controlling costs and planning the optimum utilization of network resources (Verma 94). There are two opposing methods on recovering network costs (Paradi 95): *centralized cost accounting*, where top management (e.g. County Office of Education) treats network operations as a single cost center, or *end-user cost accounting*, where network operations is treated as a profit center.

In the *centralized cost accounting* approach, network operations is treated as a single fixed cost or overhead and subscribers do not share directly in the cost of the network. An example would be when the County Office pays all costs of the Network. This scheme has some drawbacks. It has been shown (Paradi 95) that there is significant wastage of resources, hogging of resources by some subscribers at the expense of others, and poor decisions made on the use of resources since there is no fiscal incentive to guide

decision making. When there is no incentive for cost reduction, unprofitable investments detrimental to the organization are more likely. Nevertheless, the main advantage of the centralized cost accounting approach is that it is simple to administer.

The *end-user cost accounting* approach is consumption-based and involves the sharing of network costs by billing network subscribers (schools and organizations) directly ("chargebacks"). Chargebacks can be computed from simple division of total cost equally among subscribers, charging subscribers strictly according to usage, or most often some combination of the two. Research suggests (Willits 85) that if price or chargeback of network services is based on actual costs, then accurate cost allocation must be performed. This requires identification of specific *fixed costs* (costs that are insensitive to amount of usage) and *variable costs* (costs that vary directly with usage). Network subscribers share *fixed costs* equally and each are charged directly for their own *variable cost*.

Actual network *variable usage* must be measured by a network management system. A common metric used to measure consumption of network resources is the number of 256-byte packets transferred through a given interface. Other variable cost metrics are: processing time (milliseconds) for shared processing, megabyte-hours for shared data storage, and number of lines for shared printing (Paradi 95).

Fixed network costs include equipment and hardware, building, utilities, and staffing, service provider charges (if on a fixed, monthly rate) and telecommunication provider charges (if on a fixed, monthly rate).

Total cost based on the sum of *fixed cost* and *variable costs* (Figure 6.16), must be computed separately for each network subscriber. The charge for each subscriber is based on total cost.

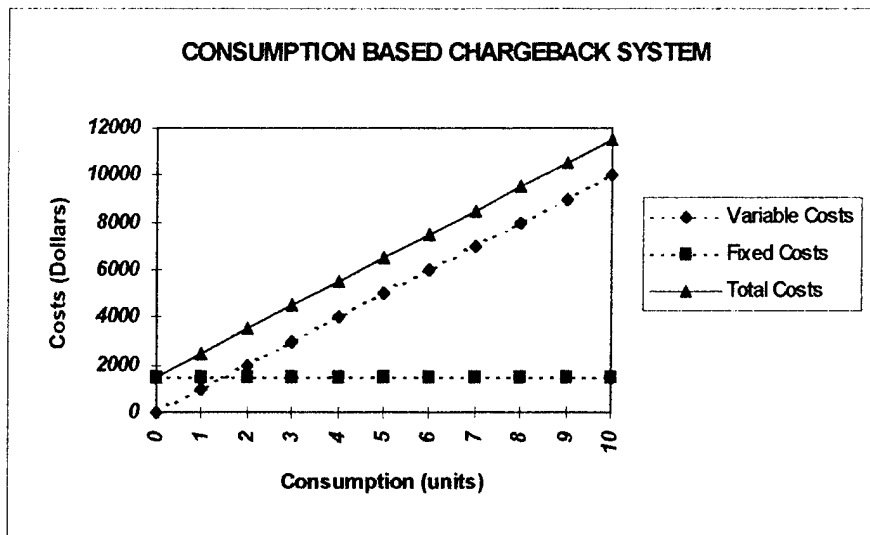


Figure 6.16 Fixed, variable and total costs.

Some (Bergeron 86) cite the advantages of imposing a consumption-based chargeback system to discourage wastage of network resources because with adequate cost information, subscribers can modify wasteful consumption by making cost cutting decisions. A network management system is essential in the fair and efficient sharing of resources regardless of the network charging method used. Additionally, the response of users to the chosen cost allocation method must be considered.

...viewing charging purely as a cost allocation mechanism fails to recognize that charges have a direct influence on user attitudes, behavior, and decisions, and that the main motivation underlying charging is usually to control computing activities through this influence on users. Charging will only be fully effective if these underlying management control objectives are explicitly considered in designing the charge-out system, so as to ensure that the desired influence does occur (Bernard 77).

Others argue that direct charging of subscribers for network services discourages utilization of these services (Quinlan 89). Furthermore, detailed cost accounting appears contrary to an educational mission which encourages free, open, and innovative network by educators and students. In the case of Monterey BayNet, the variable usage metrics appear neither necessary nor desired. The sites purchase their own hardware and flat rate Frame Relay service from Pacific Bell. The remaining network administration costs (Network Operating Center, Network Information Center, network servers etc.) are fixed in nature. These fixed costs can be divided equally among the sites. The benefits of this charging scheme is that it presents an economy of scale. The cost of the network does not rise proportionately with the number of sites. A fixed cost divided by more sites means lower charges per site.

A network accounting data base is required to support a chargeback system. Items maintained include sites, site administrators, addresses, e-mail, and phone numbers. It soon becomes apparent that a big disadvantage of a consumption oriented charging system is that it requires significant cost to administer (Emery 87). In some cases, this cost may preclude its use in favor of charging methods that are easier to administer. RFC 1272 cites the chief deterrent to usage reporting is the cost of measuring usage which includes three components listed in Figure 6.17.

- Reporting/collection Overhead (also adds additional computing, traffic and storage loads).
- Post-processing Overhead (reports, bills, collect revenue, etc.).
- Security Overhead (mechanisms to protect from disclosure and manipulation).

Figure 6.17 Deterrents to usage reporting (RFC 1272).

The costs of a complex network accounting system far outweigh any of its benefits when evaluated against the educational mission of K-12 schools and is not recommended for Monterey BayNet.

3. Other Uses of Network Accounting Information

Last, network accounting management may include managing input for network software services. Stanford University Network (SUNet) and Bay Area Research Network (BARRNet) use a system called NetDB (Lynch 93) to perform this task. NetDB is a network management system built around a relational database that contains information about network components and their relationships, host names, IP addresses, networking software, locations (inventory), remote system administrator and more. This data is used as input for software services such as the Domain Name System (DNS) for creating new hierarchical hostnames, Bootstrap Protocol (BOOTP) for booting network nodes that do not have boot instructions within the device, as well as AppleTalk tables and IP routing tables for routing (Cady 95).

D. CONFIGURATION AND NAME MANAGEMENT

Configuration management includes service provisioning (assignment of services and privileges to end users) and resource provisioning (adjust resources to satisfy the expected service demand) (Aidarous 90). It is the set of capabilities "that exercises control over, identifies, collects data from, and provides data to remote agents to assist in the continuous operation of interconnection services" (Sugarbrood 90). Among these capabilities are maintaining, adding, or updating network components and links.

Configuration Management is a primary network management function because it is responsible for putting the network in place. It also fine tunes the configuration for delivery of services to specific customers and databases. Finally, it establishes a resource database and maintains resource status for use by other network management functions (Aidarous 94).

Configuration management is required because a network is composed of many different components that can be linked together in a very large variety of ways. A continuous proactive decision-making process is required to monitor and maintain optimum network configuration. Network configuration is also concerned with initializing and gracefully terminating part or all of the network. Name management is included with configuration because naming of components is closely associated with provisioning and configuring of individual components of the network.

School and site requirements dictate that they be informed whenever a network configuration change might affect them. They also need to be informed of the final status of changing network resources and components as well.

1. Configuration Parameters

The first aspect of configuration management considered is configuring of *network protocols*. Network protocols are conventions governing the way routers cooperate to exchange data between themselves and end-terminals (Stallings 94). Network protocols dictate network address formatting just as a letter has a standard address format to facilitate delivery through the postal system. Components must be configured with the same network protocol(s) in order to communicate.

There are two classes of network protocols: *connection-oriented* and *connectionless*. Connection-oriented protocols establish and require positive indication of a connection between parties before any data is transferred. Connectionless protocols are like delivering a letter to the postal service. The data is simply delivered to the network without any prior connection being established between parties. It is assumed that it will reach its destination, just as a letter is assumed to reach its destination when it is mailed. The most common network protocols are described in Table 6.3.

By far the most popular, most ubiquitous and widely used of the network protocols is IP (and related protocols, ICMP and ARP). Because of these factors, its simplicity, and adequate functionality, IP is the sole network protocol of Monterey BayNet. Initial thoughts of using additional network protocols were rejected by group consensus because any additional performance and functionality gained would be more than offset by the large amount of effort required to configure and maintain multiple protocols.

NETWORK PROTOCOLS

| PROTOCOL | DESCRIPTION |
|------------------|--|
| IP | The Internet Protocol is a connectionless protocol that uses addresses of 4 octets. The data packet has source and destination addresses, reassembly information and some routing options. |
| CLNP | (connectionless Network Protocol) is derived from IP. It has variable length addresses up to 20 octets. |
| X.25 | a connection oriented protocol. It has a call setup packet that establishes the connection and assigns all the datagrams of a given session a "transaction number" and receipt of each packet must be acknowledged. |
| ARP | (Address Resolution Protocol) is IP's network layer neighbor discovery protocol. It works with ICMP and allows new nodes to be attached to the network, automatically be identified and all the network components updated with knowledge of the new node. |
| ES-IS | (End System to Intermediate System) is ISO's neighbor discovery protocol. |
| DECnet | Digital Equipment Corporations proprietary Digital Network architecture, known for congestion control and performance features. |
| IPX | (Internetwork Packet eXchange) Novell's NetWare proprietary protocol that connects Novelle NetWare clients and servers. |
| AppleTalk | Apple Computer, Inc. proprietary network protocol for communication between apple products and other computers. |
| SNA | (Systems Network Architecture) IBM's proprietary network protocol used by IBM mainframe and IBM-Compatible computers. |
| XNS | (Xerox Network System) Xerox proprietary network protocol. |

Table 6.3 Network protocols (Lynch, Rose 93).

The next configuration task is to assign *routing protocols*. Routing protocols allow routers in a network to communicate address forwarding information between each other for efficient transfer of datagrams (data packets) through a network. This address-forwarding information is formatted in address tables. "A TCP/IP Tutorial"

(RFC 1180) includes 28 pages of explanation on events involved in routing IP datagrams through a network.

Routing protocols are divided into two categories: *distance vector* and *link state*. Routers that use *distance vector* protocols base datagram forwarding on the port with the fewest number of nodes (intermediate routers) to the destination. This is calculated after receiving address tables from the neighbors on each port indicating how far each of them is from the destination node. Each router in a serial train (series of consecutive routers) sends the datagram out the port with the lowest number of nodes toward the destination.

In *link state* protocol, each router determines the identity of its neighbors and number of links to each neighbor. This information is placed into a link state packet (LSP) and periodically broadcast to the surrounding routers (Lynch, Rose 93). Based upon the information in the LSP database, a route to a destination is computed and used to generate a forwarding database that will tell the router which neighbor (port) it should forward datagrams for each possible destination in the network. This forwarding database only changes if there is a change in the network. The change would signal re-computing and storing new values in the forwarding database. Thus instead of broadcasting entire address tables into the network as in distance vector protocols, in link state protocol. The LSP's are broadcast and tables are generated internally to each router. Because less bandwidth (less data) is required for link state than distance vector routing protocol, link state protocols are typically more efficient for larger networks.

Networks can be partitioned into subnetworks called *autonomous systems*. Protocols that route *between* autonomous systems are called interdomain routing

protocols. Protocols that route *within* autonomous systems are called intradomain routing protocol. The most common routing protocols are described in Table 6.4.

ROUTING PROTOCOLS

| PROTOCOL | DESCRIPTION |
|--------------|---|
| RIP | (Routing Information Protocol) is a distance vector routing protocol for IP. Variants of RIP are used to route XNS and IPX. |
| IGRP | (Interior Routing Gateway Protocol) is a CISCO proprietary intradomain routing protocol, a distance vector protocol. |
| EGP | (Exterior Gateway Protocol) is the original <i>interdomain</i> routing protocol for IP, a distance vector routing protocol. |
| IGP | (Interior Gateway Protocol) is an <i>intradomain</i> routing protocol for IP, a distance vector routing protocol. |
| BGP4 | BGP4 - (Border Gateway Protocol) is an interdomain routing protocol for IP that is the replacement for EGP. |
| IDRP | (InterDomain Routing Protocol) is an interdomain routing protocol for IP with more functionality than BGP. |
| IS-IS | (Intermediate System to Intermediate System) is a link state routing protocol designed for OSI networks. |
| OSPF | (Open Shortest Path First) is a link state protocol designed for TCP/IP networks. |
| GGP | (Gateway-to-Gateway Protocol) is a distance vector routing protocol, also the first Internet routing protocol. |
| RTMP | (Routing Table Maintenance Protocol) is Apple Computer's proprietary distance vector routing protocol. |

Table 6.4 Routing protocols (Lynch, Rose 93).

After considerable discussion on the advantages and disadvantages of the routing protocols, the I³LA Net Design tiger team decided to implement IGRP as the routing protocol for Monterey BayNet (Bigelow 95). Cisco routers were chosen to "populate" the network. IGRP, their proprietary routing protocol, is preconfigured and simpler to implement on their products. OSPF is good in large networks where bandwidth overhead

must be minimized. OSPF was seriously considered but Monterey BayNet is moderate in size and routing protocol traffic is not expected to be significant. IGRP was chosen because it is simple to configure and easy to maintain (Bigelow 95).

Besides network and routing protocols, other configuration parameters for the network are the variety of media and interface connections. All these must be included in the router configuration. For example, on the Local Area Network (LAN) side, Ethernet/802.3, token ring/802.5, or FDDI may be specified along with the specific interface and the address of that interface (or port). On the wide-area network (WAN) side, configuration settings might include synchronous serial (T1/T3), Frame Relay, or ATM (SONET) and associated interface information (Monterey BayNet uses all three). In addition, each of these technologies has its own unique subset of configuration parameters.

Configuration management includes the ability to remotely identify network components and query them for information on their configuration status. Each of the routers in Monterey BayNet has an assigned router name (which is also used in the router's command line prompt), a "virtual" (read-only) password, an "enable" (read-write) password, at least one serial (WAN) port address, at least one ethernet (LAN) port address, and some have up to 16 asynchronous dial-in port addresses. Almost all of the above information is required to access and reconfigure a single router. It becomes rapidly apparent that some form of assistance will be necessary when a configuration change in the network requires flawless updates to hundreds of routers.

There are many of methods for actually maintaining and updating component

configurations and relationships. At this writing, some configuration methods for routers (servers are similar) include:

- At each site, connect to the router console port with a laptop (or desk top) and modem software, insert passwords and settings. This method is termed "out of band" because it does not use the information carrying signal paths nor capacity (bandwidth) of the router.
- Use *telnet* to access the router through the serial (WAN) port from a remote site, and insert configuration changes. It is important to note that some changes may require a reboot of the system, and if not inserted properly, local reboot at the site will be required. This method is "in-band".
- Use a workstation on the LAN that the router is serving to enter configuration commands "in-band" through the router LAN (i.e. Ethernet) port.
- Access the router over a telephone line "out of band" through a modem port from a remote workstation and modem software. This is useful when the router must be rebooted locally.

Figure 6.18 Router configuration methods.

Network management systems typically have a database containing the configuration parameters of all network components. IBM's SystemView NetView/6000 (IBM NetView Users Guide 93) automatic discovery feature retrieves the following from nodes automatically: equipment description, equipment ID, forwarding status (whether this component acts as a gateway to forward datagrams or an end-station) , IP and non-IP address tables, interface table (interface entries by number), location of equipment, and point of contact information. For each node, some of these data entries can be

- Interface Configuration
 - a. name and index of interface (Serial 0, Ethernet 1)
 - b. type of interface (Ethernet, FDDI)
 - c. maximum packet size
 - d. status of the interface (up, down)
 - e. total packets in, erroneous packets in
 - f. total packets out, erroneous packets out
- Routing Table Configuration
 - a. destinations (and default destination)
 - b. next gateway to each destination
 - c. type of connection to each destination (direct, remote)
 - d. interface to reach each destination
- Address Resolution Protocol (ARP) Table
 - a. name or IP address of destination
 - b. link address of destination
 - c. interface name of the next node to destination
- Service Configuration
 - a. service protocol (TCP or UDP)
 - b. port of service
 - c. service receiving (SNMP, TELNET, unknown)

Figure 6.19 Network node configuration parameters (IBM 93).

decomposed (Figure 6.19) on demand for more information.

Configuration management also includes *route filtering* and *traffic filtering* (Lynch, Rose 93). Descriptions follow.

Route filtering is the selective screening of routing table updates received between routers. This can be done to prefer (or deflect) routing information received from multiple external peers to pass traffic around (instead of through) a given network to optimize use of bandwidth within the affected network. Route filtering can also be

used to prevent potentially incorrect routing tables from end-user sites from being further propagated. Erroneous routing tables can otherwise result in lost or significantly delayed data.

Traffic (packet) filtering is the selective screening of user datagrams based upon some predetermined criteria. Sometimes also called "Address Firewalling", it may be particularly applicable to Monterey BayNet, where it is desirable to restrict some Internet sites from the network or workstations to prevent K-8 children from exposure to inappropriate material (Bigelow 1995). This approach is untested and is the subject of intense technical debate. Traffic filtering might also be used to restrict or limit the ability of a specific workstation to send or receive. In this manner, certain workstations might be designated to send traffic and others to receive traffic.

2. Name Management

The Domain Name System (DNS) provides for the translation between hostnames (e.g. nps.navy.mil) and addresses (e.g. 131.120.254.52). It is a set of protocols and distributed databases (domain nameservers). In July 1995, the database was distributed over more than 110,000 zones with over 4,852,000 hosts and 22.6 million users (McKinney 95). DNS is a hierarchical naming system with eight generic (functional) domains and one geographic (country) top-level domain for each country in the world. The country top-level domains are derived from the ISO 3166 two-letter country code and are listed in Appendix A (Fielding 94). The six generic codes are shown in Table 6.5. One level or tier below, the top-level domains are divided into subdomains, and

| Domain | Contents | Example |
|--------|--------------------------|------------------------|
| COM | US Commercial | cisco.com |
| EDU | US Educational | monterey.edu |
| NET | Network | es.net |
| MIL | US Military | nps.navy.mil |
| GOV | Other US Government | nasa.gov |
| ORG | Non-Profit Organizations | mbari..org |
| ARPA | Old Style Arpanet | ito.arpa.mil |
| INT | International | Used by NATO |
| NATO | NATO Field | Being replaced by .int |

Table 6.5 Top-level domains (Lynch, Rose 93) (Fielding 94).

each subdomain is divided into numerous sub-subdomains, etc. This hierarchical structure forms a triangular collection of nodes under any chosen node. The triangular area under the selected node is called a "zone" and each zone has an owner. For example, if another school wants to join the domain of "monterey.k12.ca.us", they would contact the person at the Monterey County Office of Education (MCOE) and get permission. The Monterey County Office of Education had to get permission to join the "k12" domain. The person who owns the "k12" domain had to get permission to join the "ca" (California) domain. Similarly the "ca" domain is part of the "us" (United States) domain.

Proper formulation and assignment of host names and addresses is vital in the ability of users to communicate across the network. There are several tasks that must be completed when adding any new component (host) to Monterey BayNet shown in Figure 6.20 (Bigelow 95)(RFC 1480).

- Decide on a hostname, consistent with the scheme used to assign other hosts in the same domain. RFC 1480 (The US Domain) contains guidance on the United States domain. The domains of Monterey BayNet are 'monterey.k12.ca.us' and 'santacruz.k12.ca.us'. Schools, district and county offices of education and are "k12" sub-domains. Hosts are individual workstations, servers, printers, etc. at those facilities. Other subscribers to Monterey BayNet such as libraries (.lib), businesses (.com), research organizations (.org), and military (.mil) fall under different subdomains from the "k12" subdomain.
- The network nodes or host are registered by filling out a U.S.Domain Template per RFC 1480, and sending it to the U.S. Domain Registrar (us-domain@isi.edu).
- When approved, the name is configured into the appropriate routers, and nameservers of the network. The Internet service provider is notified in the event that updates are needed are needed for service provider nameservice equipment.

Figure 6.20 Hostname registration and assignment (RFC 1480).

"Requirements for Internet hosts - application and support" (RFC 1123), "Domain Names-Concepts and Facilities"(RFC 1034) and "Domain names-Implementation and Specification"(RFC 1035) contain additional detailed information on the Domain Name System and managing names in a network.

Although domain names are easier for people to remember and use, IP (Internet Protocol) addresses are the operational addresses used by machines (Cady 95). They must be obtained and distributed to the schools and organizations in the network.

Obtaining IP addresses is a separate activity from assigning domain names. The network manager contacts the Internet service provider (CSUnet, BARRnet) or other regional registration authority. This information can be obtained at the central Internet Registry at Hostmaster@INTERNIC.NET (RFC 1480).

Name management includes generation of host tables for domain name service for the domain and entering them into the domain nameserver. These tables include domain names, their corresponding IP addresses, reverse IP addresses (fields inverted), and information on root name servers. Whenever a new school is added to Monterey BayNet, network management personnel must add information on that school to the files in the domain nameserver that will allow identification and delivery of data to and from that school.

Last, name management includes the generation of BOOTP (Boot Protocol) Tables. Bootstrap Protocol allows a diskless client machine to discover its own IP address, the address of a server host, and the name of a file to be obtained, which is then loaded into memory and executed (RFC 951). This allows diskless workstations to reboot automatically off a network server after a power outage, for example. The network manager maintains the BOOTP tables current with network names, IP addresses, boot file names, paths, etc.

E. PERFORMANCE MANAGEMENT

Performance management consists of continuously evaluating Monterey BayNet component utilization and making adjustments to optimize that utilization. The overall

overall objective of network performance management is to ensure that there is enough capacity (bandwidth) to support school and site requirements (Held 92). Thus, performance management is closely associated with capacity planning.

Performance management includes functions to gather statistical information, maintain and examine logs of system state histories, determine system performance under natural and artificial conditions, and alter system modes of operation for the purpose of conducting management performance management activities. (Aidarous 93)

Khanna, Lloyd, and Yundt cite three activities of a network manager in performance management (Lynch, Rose 1993):

- Monitoring the network (gathering statistics).
- Analyzing the data (trend analysis or baselining).
- Adjust topology or key parameters in network devices or servers to remove

Figure 6.21 Performance management activities (Lynch, Rose 1993).

One of the most important jobs in the network management process is to determine the performance of network equipment and circuits (Held 92). With this data, forecasts can be made that will project when the capacity of currently installed equipment or circuits will be exceeded. Performance data can also help to locate bottlenecks, isolate the causes of congestion (excessive traffic buildup), or determine when a portion of the network with excessive capacity might be used to support another overloaded part of the network.

1. Performance Monitoring

The most basic consideration in evaluating or monitoring network performance of Monterey BayNet is network *bandwidth*. It is technically the difference between highest and lowest frequencies of the transmission channel, and is directly proportional to the number of bits per second (bps) that the channel can transfer. The bandwidth limits the theoretical maximum data flow rate the channel can carry, no matter how efficiently the network is configured. Table 6.6 gives relative speeds of a typical e-mail message of 2.2KB size. Routing delays are not included.

| RATE/BANDWIDTH(min) | TRANSFER TIME | IMPROVEMENT |
|---------------------|-----------------|-------------|
| 2400 bps / 4800 Hz | 7.3 seconds | Y |
| 9600 bps / 19200 Hz | 1.83 seconds | 3.98 x Y |
| 19200 bps/ 38400 Hz | 0.916 seconds | 7.96 x Y |
| 56 Kbps / 112 KHz | 0.314 seconds | 23.24 x Y |
| 1.5 Mbps / 3.0 MHz | 0.0113 seconds | 646.01 x Y |
| 45 Mbps / 90.0 MHz | 0.00039 seconds | 1871.79 x Y |

Table 6.6 Relative speeds of an e-mail message (Cady 95)

Bandwidth in Table 6.6 is calculated from the data rate using the Nyquist sampling theorem (Freeman 91). This provides the network manager a crude, first-order estimate of bandwidth required for a given data rate. It also gives a convenient method of calculating bandwidth margin left. As more complex resources and network applications become available to Internet users, and as the number of users increases, the demand for network bandwidth is increasing exponentially (Lynch, Rose 93). RFC 1296 discusses the growth of the Internet from 1981-1991.

Four network performance criteria are used to measure the status of a network: *response time*, *throughput*, *utilization* and *availability*. Discussion follows.

Response time (also called line turnaround time) is the time that it takes a datagram or signal to make a round trip along a specified path (Held 92). To the user, a long response time appears as if there is a long delay between hitting the "enter" key and getting a response back. Congestion (traffic queuing) due to traffic overloads can cause delays and long response times. Faulty repeaters or routers can also cause processing delays and long response times. Misconfigured devices such as incorrect routing tables or overloaded servers can also cause long response times. Long response time is an indication that there is a problem present which needs further investigation. IBM's NetView Performance Monitor and the Frederick Engineering FELINE protocol analyzer both include tools for network management personnel to measure response times (Held 92). *ping* (discussed earlier) can also be used as a tool to sample response times also.

Throughput of a data channel is an expression of how much data can be transferred, and is also an expression of channel efficiency (Freemen 91). RFC 1242 defines "throughput" as "the maximum rate at which none of the offered frames are dropped by the device" (RFC 1242). The important thing about this definition is that it does not allow for dropped packets because when a packet is dropped, transmission is stopped until the higher level protocol recognizes that the packet is missing and requests re-transmission. It is obvious that the delay at this point (in seconds) can have a major effect on the value of throughput (Lynch, Rose 93) with the resulting value

much lower than the channel normally produces. The ultimate effect of an offered frame rate faster than the throughput of a connecting device is dropped packets! The percentage of dropped packets increases with the mismatch between offered frame rate and throughput. Poor throughput can be caused by high traffic density (congestion or small margin of bandwidth left for additional efficient transfer of data), dropped packets (requiring more bandwidth and delays for re-transmission requests and acknowledgements), or inadequate server buffers or disk I/O bottlenecks (prevent the complete and efficient transfer of data to the buffering location for further processing). Sometimes a condition resulting from the cycling between dropped packets and retransmission requests for those increasing number of dropped packets causes a positive feedback condition called a *broadcast storm*. "Congestion Control in TCP/IP networks" (RFC 896) discusses the effects of congestion and broadcast storms on network performance and some corrective measures. Needless to say, throughput is extremely poor in the presence of a persistent broadcast storm and intervention from network management personnel is usually needed to restore stability to the network.

Utilization is a measure of network efficiency and is given in Equation 6.1.

$$Utilization(\%) = \frac{Throughput}{Capacity} \times 100\% \quad (6.1)$$

If capacity represents maximum number of total bits for 100% use of a transmission medium, and throughput is the actual number of information bits per unit time, then percent utilization represents the percentage of the line that is being used. In analyzing

percent utilization represents the percentage of the line that is being used. In analyzing utilization, values greater than 75 % usually indicate a performance problem (Held 92).

Availability is the last and most important aspect of network performance management. It represents a measure of performance from a high level view, and embodies, in essence, a summary of all the other factors. Network managers report it on some periodic basis in terms of percent "up time." In cases of global outages or complete system failures, it is fairly straight forward to compute. However, marginal-to-poor performance is more difficult to assess in terms of percent up time.

2. Operational Monitoring

To proactively manage a telecommunication network like Monterey BayNet, it is not difficult to see that an automated network management tool in a Network Operating Center is essential. Continuous monitoring of link status and data flows, link error rates, and router status with an automated network management system can provide the pre-alertment capabilities required to identify, diagnose and correct both performance problems and faults before they have a significant and noticeable impact on the system. This support is very important for the school teacher who relies on the network to deliver elements of an interactive lesson plan, or the school administrator who needs to obtain a student's record to make an important decision.

Without a network management system and a Network Operating Center (NOC), the tools required to troubleshoot are limited to the manual methods such as *ping*, *traceroute*, and *nslookup*. The limitation of these manual methods is that they require

lots of manual input to get enough output to be useful. The time required to obtain this information precludes a proactive role in fault management. Another limitation is that manual methods often signal that a problem exists but there is no indication of the location of the problem (link or node).

a. Simple Network Management Protocol (SNMP)

Given the explosive growth of the Internet (Figure 6.22), it became clear in 1988 that manual tools and a small number of network experts were insufficient to solve network management problems. When it was determined that the growth in the Internet was exponential, a decision was made by the Internet Activities Board (IAB) to develop a network management protocol. After consideration of many possibilities, the Simple Network Management Protocol (SNMP) was selected (Amatzia 90). SNMP represented an enhanced version of its precursor, Simple Gateway Management Protocol (SGMP). SNMP actually refers to a collection of specifications that includes the SNMP protocol itself, the definition of a Maintenance Information Base (MIB) database, and associated concepts (Stallings 93). RFC 1157 discusses a Simple Network Management Protocol (SNMP) including some of the history behind its development. RFCs 1441 through 1452 discuss different aspects of SNMP version 2.

Number of Internet Hosts (exponential)

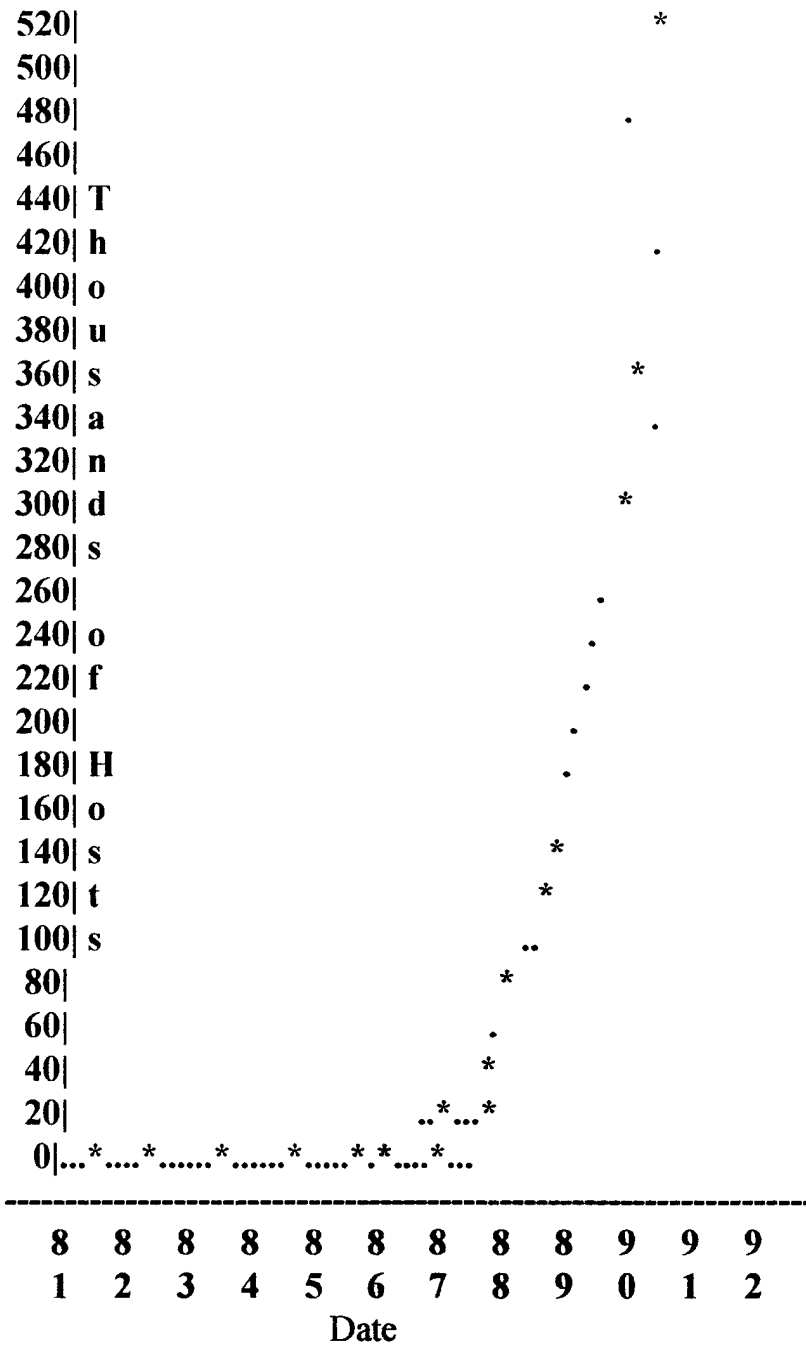


Figure 6.22 Internet Growth (1981 - 1991) (RFC 1296, January 1992)

The basic idea of SNMP network management involves the relationships of four key elements:

- Management Station
- Managed Agent
- Management Information Base (MIB)
- Network Management Protocol

Figure 6.23 SNMP key elements (Stallings 93).

The management station and each of the managed agents has a database called a Management Information Base (MIB). A management information base is essentially a collection of data tables. The names of the tables and the fields (column labels or "objects") are specified in "Management Information Base for Network Management of TCP/IP-based Internets" (RFC 1156). These objects are standardized to provide interoperability between the management station and any agents that comply with that standard, regardless of the manufacturer. A network management station executes management applications to monitor and control network agents. Network elements are hosts, gateways, routers, terminal servers etc. that contain management agents responsible for performing the functions requested by the network management station(s). SNMP is used to communicate management information between the management stations and the agents in the network elements (Fig 6.24). The basic unit of

exchange is the "message", made of an outer wrapper (community name) and an inner protocol data unit (PDU). The community name is a simple authentication scheme that

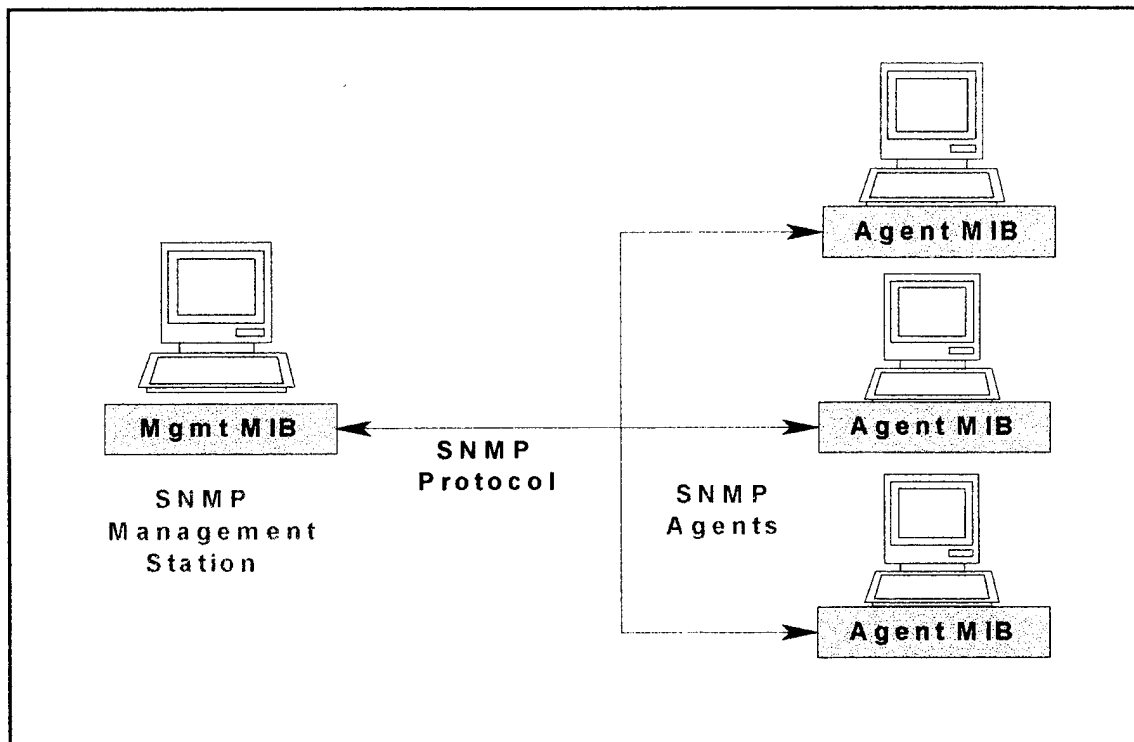


Figure 6.24 SNMP architecture.

allows an agent to recognize a message only from the network management station with the same community name. The PDU is the "meat of the message" and contains the functional parameters (data and control information) of the message.

Per RFC 1157, the strategy implicit in SNMP is that monitoring of the network state is accomplished by the network management station polling for the appropriate information. The management station is designed to interact with the agents in the network devices in only two ways. It can retrieve and inspect a value in the agent's MIB

with the "*Get*" operation, or it can alter a value in the agent's MIB with the "*Set*" operation. Under certain conditions, a remote agent can present values from its MIB to the management station unsolicited, called a "*Trap*" operation.

Imperative commands for an agent device to perform some action are excluded from the set of management functions. A benefit of the decision to limit management functions to GET and SET is to avoid introducing support for an ever-increasing number of imperative commands into the protocol and making it arbitrarily complex. The indirect methodology by which an SNMP manager accomplishes desired effects without commands in a given agent can be described by the following analogy.

The remote agents' MIB can be thought of as that agents' way of seeing the network. The agent responds and acts only on information that it sees in its MIB. The network management simply polls the agent (GET), inspects the contents of its MIB and sends out a changed value to some parameter in the MIB (SET). The agent now responds to the changed value in its MIB. For example, rather than implementing a direct "reboot" command, a reboot can be invoked by setting a MIB parameter called "number of seconds to reboot" (RFC 1157).

SNMP operates only with unreliable datagram service (UDP) to minimize impact of the network management system on network capacity (bandwidth) and to comply with the SNMP goal of simplicity.

b. Operational Limitations of SNMP

"The heart of the SNMP framework is the simple network-management protocol itself. The protocol provides a straightforward, basic mechanism for the exchange of management information between manager and agent" (Stallings 93). SNMP's greatest strength is also the source of its greatest limitations as enumerated in Figure 6.25 (Lynch, Rose 93).

Open System Interconnection (OSI) has addressed many of these deficiencies in its versions of a network management system (Yemini 93). OSI network management architecture uses CMIS (Common Management Information Service) to define numerous commands or procedure calls with parameters. The OSI protocol CMIP (Common Management Information Protocol) specifies the format of the Protocol Data Units (PDU) for each of the commands. OSI also uses connection-oriented transport for confirmed interactions (Amatzia 90). Nevertheless, given the sheer size and complexity of OSI network management protocols, some see the cure as being worse than the disease (Stallings 93).

To reduce monitor traffic and provide for a more efficient network performance scheme within SNMP, it may be possible to combine SNMP polling to monitor agents, and link-state information from a link-state routing protocol such as OSPF or IS-IS to monitor the state of network links (Stallings 93).

Since SNMP relies heavily on polling ("get" requests) and since "traps" are few in number, it is important to limit the impact that network management system has on

- The suitability of SNMP decreases as the size of the network increases. This is because the managing station must send out a packet to get back one packet of information. A large volume of polls for a large number of agents may yield unacceptable response times at the user application level.
- SNMP is not designed to retrieve a large quantity of data with one poll, such as an entire data or routing table.
- Because UDP/IP is used to deliver messages, an agent cannot be sure that a critical trap message has reached the management station (Lynch, Rose 93).
- SNMP provides only trivial authentication (community name).
- SNMP does not support imperative commands, but triggers events in agents indirectly, by setting an objects value. This is less flexible than other approaches with can send commands and arguments
- SNMP MIB is limited and doesn't support sophisticated queries.
- SNMP doesn't support manager-to-manager communications or a mechanism where a manager can learn about devices managed by another management system (Park 93).
- SNMP cannot tell the difference between the loss of many downstream agents due to a single failed link and the loss of all the agents themselves (Lynch, Rose 93).
- With some routing protocols that can propagate tables rapidly throughout the network, it is possible to reroute the traffic around a failed component between SNMP polls, masking the failed component.

Figure 6.25 Limitations of SNMP(Park 93) (Stallings 93)(Lynch, Rose 93).

the network. Network management staff can accomplish this by regulating the polling interval. If the polling interval is set too long, then delay of the network management program to problems may be unacceptable. If the polling interval is set too short then the response times may increase and sluggishness in performance of applications may be

unacceptable to users (Eckerson 92). An approximation for the polling interval is given using Equation 6.2 (Stallings 93):

$$N \leq \frac{T}{\Delta} \quad (6.2)$$

where N = number of manageable devices or agents

T = desired polling interval (successive polls to the same agent in seconds)

Δ = average round trip *ping* time per poll (seconds) from Figure 6.10

An example is presented to illustrate how Equation 6.2 can be used to calculate the polling interval from the round trip ping time and the number of devices in Monterey

BayNet. An average of 50 devices per school is assumed for 200 schools.

$N = (200 \text{ schools} \times 50 \text{ devices per school}) = 10,000 \text{ devices}$

$\Delta = 76 \text{ ms} = 0.076 \text{ seconds (round trip } \textit{ping} \text{ time)}$

From Equation 6.2,

$$T (\text{sec}) \geq \Delta N$$

$$T \geq (0.076)(10,000)$$

$$T \geq 760 \text{ seconds} = \underline{12.67 \text{ minutes}}$$

Therefore, to support 10,000 devices, the polling interval must be 12.67 minutes or greater. This means that it could be almost 13 minutes for a fault condition in an a managed agent to be detected by an SNMP polling or "Get Request" operation. It is for this reason, among others, that SNMP "Trap" operations are sent to the network management station from the affected agent at the time of the fault instead of the agent waiting to be polled.

3. Operational Management Reports

There are many beneficial functions of reports. The most important of these is that reports serve as a formal method of structuring monitoring activities, since parameters are inspected as they are collected for the report. Second, reports are a formal means of communication between network staff and managers. Last, reports constitute a historical record from which long term trends may be detected. Log keeping is very familiar to naval crew members operating ships at sea where reporting requirements on every piece of equipment include hourly monitoring and trend analysis CERFnet has a summary report that contains the sections and information:

WEEKLY Network Summary Report:

- Header - period of report, filename and FTP address, CERFnet point of contact.
- Outages - site(s) where outage occurred, start time, stop time, reason.
- Network activity -lists chronological log entries of times and locations of congestion, routing problems, and corrective actions taken by staff.
- Communication link utilization - a table that lists the link, line speed, capacity and peak hour.
- Equipment up-time (router) since last bootup.

Figure 6.26 CERFnet weekly network summary report format (Lynch, Rose 93).

The NASA Science Information (NSI) Operations Center, at the Ames Research Center, Mountain View, California, utilizes a daily report and a monthly report shown in Figure 6.27.

DAILY Report (Action based)

- Status of Open Trouble Tickets (active or unresolved problems)
- Routed internally

MONTHLY Report (Statistically based)

- Network Upgrades
- Sites Added / Sites Deleted
- Status of Backbone Sites
- Total number of Trouble Tickets for the month
- Number of tickets from each reporting source
- Outage type (Planned / Unplanned)
- Minimum Time to repair
- Breakdown of responsible organization (NOC, site, carrier, or service provider)
- Escalation status of active tickets
- Availability (percent "up-time")

Figure 6.27 NASA Science Internet (NSI) report formats (Kamerdze 95).

F. SECURITY MANAGEMENT

Before the topic of security can be discussed, it is important that there is an explicit identification and understanding of what is being "secured." Certain information has value and inherent worth (Birch 92). In a business, if an automated inventory system helps a retail store order goods as they are purchased so that there is never a need to pay inventory costs to store excess goods, then the information is worth the cost savings that are incurred otherwise. In education, information is valuable because it leverages our understanding of the universe around us, and contributes to our ability to make wise and strategic decisions in a reasonably short time. The value of information becomes apparent when an organization is suddenly denied access to information.

Information is valuable because it can be used to increase revenue and reduce costs. When denied to others, it can be used to gain a position of power or a competitive advantage.

Not all information has the same value, and much information may be worthless. Network security of Monterey BayNet has meaning only in context of the value of the information that the network moves.

1. Network Security Management

Network security has many definitions. "Its aims are to ensure the protection of resources by preventing unauthorized access to them and monitoring exceptional states such as unauthorized access attempts" (Moffett 90). Network security typically permits only secured and authorized access to the network management system and resources (Lo 91).

Network security management can be seen as the provision of network security services for schools and sites and is the key to guarding against "denial of service" attacks by outside network saboteurs. It has five distinct components (Wallis 93) as shown in Figure 6.28.

2. Deciding on the Degree of Network Security

There are specific solutions or implementations for each of the five components of network security in Figure 6.28. The degree of implementation depends upon two factors that are determined before investing in security services. As stated before, the first item to be determined is a qualitative estimated value of the information. What will it cost the

- Authentication Services - provides a system to verify to the receiver the identity of the sender of information.
- Non-repudiation Services - provides a way to prevent a sender from falsely denying that data was sent, or a receiver from falsely denying that data was received.
- Integrity Checks - provides a way to detect the unauthorized modification of data.
- Confidentiality Service - prevents the unauthorized disclosure of information and is the service most often associated with encryption.
- Access Control - provides the means to grant or deny access to information.

Figure 6.28 Components of networks security management (Wallis 93).

school, organization, or County Office of Education if the information is compromised, lost, changed? If the information was essential to a function of the organization, what will it cost to be reproduced?

The second thing to determine are the various threats to security and their probability of occurrence, called a *risk assessment*. Qualitative and quantitative methods exist to compute and assign a dollar value to the sum of various losses and their probabilities (Birch 92).

The criteria for spending on security systems is based on the result of the risk assessment. The security afforded to the system ought not exceed the dollar loss value calculated in the risk assessment. A good end-to-end public-key encryption system can accomplish the first four objectives, authentication, non-repudiation, integrity and confidentiality, but at a considerable monetary expense and prohibitive administrative

confidentiality, but at a considerable monetary expense and prohibitive administrative expense. It will also slow applications due to the extra processing power and bandwidth that will be added by the encryption-decryption process. Is the value of information in the network worth the costs in security, administrative overhead and performance?

A reasonable amount of security for the value of the information on Monterey BayNet can be probably afforded by the last security service, *access control*. The most common form of *access control* is the use of a *login* and *password* system. If used correctly, this can be effective for most purposes in Monterey BayNet. In addition, "in band" attacks (invasion on the normal data links from sources outside the network) can ordinarily be prevented by the use of "firewalls" at a single point of entry into the network.

A firewall is a device installed in a single entry line connecting the LAN at the subscribing site to Monterey BayNet that forces all datagrams to be examined and evaluated (Wack 94). It is essentially an "intelligent" filtering device. There are many different types of firewalls and they come at many different prices. The most common are *packet filtering routers* and *application gateways*. *Packet filtering routers* can filter IP packets based on any or all of the following:

- source IP address
- destination IP address
- TCP/UDP source port
- TCP/UDP destination port

The router discards unauthorized packets after retrieving and forwarding their addresses to network management staff. *Application gateways* filter specified application level

protocols such as FTP, TELNET, and E-mail, permitting them access to the network only after certain authentication procedures are met. They can also be programmed to allow access only to designated workstations in a network.

It is important to prevent "backdoor" attacks on the network around the firewall via modem dial-in modem connections by ensuring adequate login and password protection on dial-in lines.

3. SNMPv2 (version 2)

SNMPv2 is an upgrade of SNMP that incorporates secure network management. As mentioned previously, SNMP was developed starting in 1988 as a result of the critical demand created by the exponential growth of the Internet. Initially plans were to implement SNMP immediately while developing a transitional network management protocol called CMOT (common management information protocol). CMOT was intended to bridge the gap between SNMP and an OSI-based system. Since that time, delays in development of stable OSI standard implementations left SNMP in operation (Stallings 93). SNMP is now implemented by a large number of vendors and is widely deployed. SNMPv2 has been proposed to address some of the weaknesses in SNMP(v1) and be interoperable with it at the same time (Stallings 93). Accordingly, SNMPv2 has significant improvements in functionality over SNMPv1 as shown in Figure 6.27.

- Manager-to-manager capability
- Ability to retrieve large blocks of data with one poll
- More elaborate database (MIB)
- Network security capability

Figure 6.29 SNMPv2 improvements (Stallings 93).

Security is provided between managers and agents with the addition of extra fields to the SNMP protocol data units (PDUs). In addition to the source and destination fields, a context field (a function code for a location in the a destination's MIB table where the function to be performed is described) , authentication field and access control field are provided. Thus, the protocol data units consist of an address wrapper and various codes for access, authentication and function. The access code permits the PDU to be read by the agent, the authentication code permits what was read to be "believed" and acted on, and the context code tells the agent where in its MIB to find the meaning of what was read. A network can operate in a mixed SNMPv2 / SNMP environment.

G. SUMMARY

A well-designed Network Operations Center (NOC) is result of a thorough consideration of the mission of Monterey BayNet in relation to the broader K-12 educational mission, the Agenda for Education in the State of California. At the network level, the well designed NOC achieves a balance in the five network management functional areas of fault management, configuration and name management, accounting

management, performance management and security management.

A central *fault management* system is necessary to support the K-12 education availability mission of the network by minimizing the impact of equipment failure and maximizing network uptime. To document efforts during fault recovery for future reference and automate notifications, a Trouble Ticket system is included.

Configuration and name management supports the K-12 education reliability mission by providing optimum physical topology, network and routing protocols, equipment configurations, and standardized domain names and IP addresses that are both functional and scalable.

Accounting management is needed to support the K-12 operational mission by distributing financial responsibility for the network fairly among all the network benefactors.

Performance management ensures the K-12 education quality mission not only to deliver a valuable service, but to deliver a high level of quality with it. Consistent availability, high throughput and low response times are the fruits of a high quality network management system.

Security management is needed to promote the K-12 education security mission to protect the physical and functional integrity of the network, as well as the information it stores and carries.

A network is a distributed information system, but the centralized coordinating functions of network operations, the network management station and personnel who run it are vital to the functionality and long-term sustainability of Monterey BayNet.

VII. NETWORK INFORMATION CENTER (NIC) FUNCTIONS

A. INTRODUCTION

User support through the Network Information Center (NIC) is concerned with helping subscribers and users utilize the tools that will assist them with access to network resources (CDE 94). A NIC provides administrative support, user support and information services for a network. The staff of the NIC provide help desk services. This may include being available to answer the many questions of new users, provide training in new tools and applications, and distributing information about resources about new resources on the network. The NIC staff are also available to answer more technical questions when users are having troubles running an application, printer or accessing a server.

B. CONNECTION SERVICES

One extremely important function of the NIC is to provide support for new network subscribers. This can include information on the technical aspects of the network connection, data rates and limitations that may be imposed, and how to optimize their "piece of the pipe" for their students and users.

1. Internet Service Connections

Connection from the Internet service provider (CSUnet) to the Monterey and Santa Cruz County Offices of Education are provided by a T1 (1.544-Mbps) frame relay

service to each as shown in the network topologies in Appendix B. High schools and other organizations (except K-8 schools) get 128 Kbps frame relay Internet service directly from the CSUnet. K-8 schools get 56Kbps, 64Kbps and 128Kbps Internet service through their respective County Offices of Education. The topology supports administrative traffic directly between all schools and the County Offices of Education. Currently 128 Kbps is recommended as the minimal connection speed for TSU/DSU and router scalability reasons (Bigelow 95).

2. Dial-in Service

Monterey BayNet uses Cisco 2511 routers to provide dial-in services at certain school sites and organizations that desired this capability. Dial-in access augments the principal the principal Frame Relay WAN connection. Dial-in service is an excellent, cost-effective way to add value to a school network because it is convenient. Teachers, students, parents and administrators can have direct access to Internet information services. In addition to the normal router serial port for WAN frame relay connectivity and ethernet ports for LAN connectivity, there are 16 asynchronous ports for 16 dial-in modem connections on the Cisco 2511 Router.

IP is designed to handle packet-oriented data from the link later. Serial modem connections from the phone company supply a continuous data stream instead of packets. Serial Line Internet Protocol (SLIP) (RFC 1055) and Point-to-Point Protocol (PPP) (RFC 1661) are encapsulation protocols that make the two compatible by framing the continuous data stream into packets compatible with IP (Cady 95).

The NASA Lewis Research Center NIC in Cleveland, Ohio provides an excellent example of a Dial-in Network Users Guide at

http://netgopher.lerc.nasa.gov/Guides/guides_overview.html

for instructions and information on setting up modems and accessing the network through dial-in connections (Eubanks 94).

a. Serial Line Internet Protocol (SLIP)

Serial Line IP is discussed in RFC 1055. It can support only one protocol, IP and does not support other protocols like OSI/CLNP, Novell NetWare/IPX, DECnet, and AppleTalk. Presently, in Monterey BayNet, This is not a limitation for Monterey BayNet since IP is the only network protocol. SLIP has no error detection capability, so this function must be performed by TCP or the application. There is no authentication mechanism of incoming connection (Cady 95). SLIP is useful but it has large overhead which reduces effective bandwidth. For these reasons, Monterey BayNet subscribers use PPP protocol instead of SLIP.

b. Point-to-Point Protocol (PPP)

Point-to-Point Protocol (PPP) is a serial line protocol defined in RFC 1661, which allows TCP/IP connectivity over dial-up links on a telephone line. PPP is a newer, more powerful, more complex, and more robust protocol than SLIP (Lynch 93). In order to use PPP dial-in service, the following prerequisites must be met (Cady 95):

- A remote TCP/IP-based system (PC with "Trumpet Winsock" or Mac with "MacTCP").

- A high-speed asynchronous modem.
- PPP software installed on the remote system (this comes with Trumpet Winsock and MacTCP).
- PPP userid and password, IP address and domain name of the Domain Name Server, e_mail server and Net News server.
- The default IP address

PPP Dial-in Network service is comprised of a router (Cisco 2511) and a pool of high speed asynchronous modems attached to several dial-in numbers.

The router act as an access control device between the dial-in modems and Monterey BayNet. The modem bank permits data (DCE) rates up to 14.4kbps via CCITT V.32bis as well as supporting V.42bis and MNP-5 data compression. All PPP communications require an 8 bit, no parity, 1 stop-bit link. Advantages of PPP over SLIP include the fact that PPP supports multiple protocols on the same link (more flexible), assigns an IP address dynamically to a remote device (allows mobile hosts to connect to the nearest point of network presence) instead of having to type it into a configuration file, has better data compression, and allows for authentication of the user as the connection is being established (more secure). For these reasons, PPP is the recommended dial-in protocol for Monterey BayNet Subscribers.

C. OTHER NETWORK SERVICES

The network information center (NIC) handles configuration and maintenance of network service resources. This includes keeping various servers (domain name server, mail server , web server, file server, news server) running and updated.

1. Domain Name System (DNS)

It's important to have a basic understanding of how the Domain Name System (DNS) works to develop an appreciation for the role that the NIC staff has in updating and maintaining it.

Computers address each other by number (i.e. IP address) instead of using the host naming systems that are more meaningful to people. Given a hostname, the DNS system ideally allows a host to find the corresponding IP address and access any remote host on the Internet. It might seem that a single table of host names mapped to corresponding IP addresses is all that is needed, similar to the way that names are mapped to telephone numbers in the telephone directory. This table might then be made available to every host in the Internet, with periodic updates to include additions and changes. Such a method was used until the growth of the Internet made this approach untenable.

In 1984 Paul Mockapetris of University of Southern California's (USC) Information Sciences Institute (ISI) designed a new architecture that distributed the single host name database from one location to many distributed locations or "domains," calling this system the "Domain Name System" (Albitz 95). RFC 1034 and RFC 1035 describe the DNS system. The DNS is a distributed database of names, numbers, and pointers. By analogy, the phone number of someone in New York city can be found in a copy of the phone directory held locally (in a "cache"), or in New York, the area to which the directory is applicable.

A domain name server is a program that accesses a storage area for a small part of the DNS distributed database. All the name servers in the world contain the names and IP addresses (or other number addresses) of all hosts or other components. Each local name server contains the names and addresses of all network elements in its domain unless they are kept in a name server for a subnetwork of that domain. In that case, the local name server only contains a pointer to the subnetwork nameserver which has the names and addresses of the elements in its subdomain.

The hierarchical structure of the DNS system is much like a computer directory structure that uses periods to separate the names instead of slashes. This can be seen in Figure 7.1. The domain name is built from the top (root) "." level by appending the name of the next level node to the front (left) until the last node is reached. The period at the end of the domain names indicates the root (top) level and it that makes them *fully-qualified domain names*. In addition to pointers to the next level "child-domains" below it, each node has its own collection of hosts and their IP addresses. In theory, there is at least one name server at every node that contains the IP addresses for all the addressable components at that node, and also pointers to the names servers one level below it. Each name server also has a cache to store the names and IP addresses of recent queries.

As an example, assume that a host (workstation) at the node "stl.nps.navy.mil" (Systems Technology Laboratory (STL) at Naval Postgraduate School) wants to send a file to a printer at the Monterey County Office of Education. It needs the IP address of the printer, but the workstation doesn't have it. So the workstation uses a *resolver* to query the name server at the STL node. If the local name server can't find the printer's

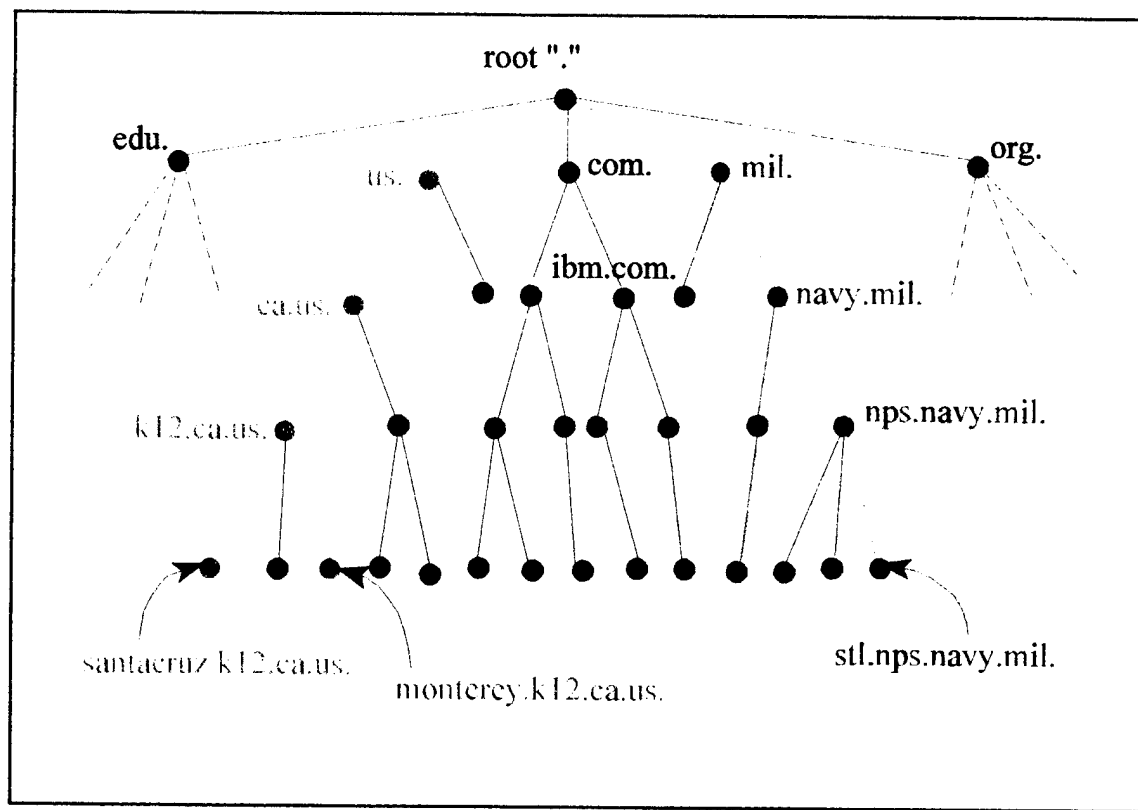


Figure 7.1 Domain Name System (DNS) Architecture (Albitz 95).

hostname in its cache, it queries a root (".") server. The root server doesn't have the IP address of the printer, so it sends back a list of domain name servers for the "us." domain. The STL name server then queries one of the "us." domain name servers. It doesn't have the address of the printer either, so it sends a list of the "ca.us." domain name servers. The process is repeated for each level down until the STL nameserver finds the printer's domain name and IP address in the monterey.k12.ca.us. name server. The STL name server can now give the workstation the IP address so that it can send the file to the printer. Information obtained by this query process down to the actual remote name server is called "authoritative." It also stores the information in a cache for an operator

specified time period, keeping it readily available in the event of subsequent transfers. If the IP address was obtained from the name server cache, it is called "non-authoritative". DNS processes queries millions of times each day in a manner that is completely transparent to users. It is crucial that the DNS is set up correctly. Without the DNS, all resolution on the Internet would eventually fail (Albitz 92).

The following criteria can be used for a site to determine whether a name server must be installed (Albitz 92). A site might consider installing a name server if:

- the site is connected to the Internet
- there is a UUCP connection to a host on the Internet
- local network is a TCP/IP based Internet
- presence of a LAN or site network

Figure 7.2 Reasons to get a domain name server (Albitz 92).

If a site doesn't have a domain name server, then its mappings must be kept and updated in another name server. The name server that retrieves domain name and address information on a host from its own internal DNS database is called the *primary name server* for that host. A *secondary name server* gets DNS data from an authoritative name server. The secondary name server is set by the operator to query the primary name server periodically to keep the secondary name server updated. The secondary name server is usually one level up in the DNS hierarchy so it will intercept queries if the primary name server is down.

Before using a local domain name server for the first time, NIC staff must first verify their block of IP addresses with *hostmaster@nic.ddn.mil* (RFC 1480). Then they register with the parent name server (this is to remove any local host names and insert the pointer to the new name server).

BIND (Berkeley Internet Name Domain) is the implementation of DNS system written for Berkeley's UNIX that is the most popular (Albitz 92). It has standard preformatted configuration files that must be configured and maintained regularly.

Although transparent to the subscribers, continuously maintaining the DNS database for Monterey BayNet is a vital part in the overall management of the network. This work must be done manually. The network cannot provide a sustainable function without it.

2. Electronic Mail

E-mail is probably the most widely used application on the Internet. Like many other network services, it requires management to function properly. To develop an appreciation for e-mail in network management and the role that the NIC staff has in maintaining e-mail connectivity, it is important to have a basic understanding of how e-mail works.

The basic protocol for transmitting mail between computers on the Internet is "Simple Mail Transfer Protocol" (SMTP) (RFC 821). In the Internet, SMTP is implemented above the reliable, connection oriented transport service, TCP/IP. SMTP describes the sequence of control messages between computers to transfer an e-mail message (Lynch 93).

Users don't interface directly to SMTP rather but go through a *mail application* which automates some repetitive functions and adds others. Eudora (for Mac or PC) is an example of a mail application which is included in the software collection for K-12 schools and organizations in Monterey BayNet (Bigelow 95). The mail application communicates with a *mailer program* through a file system (Figure 7.3). When the e-mail message is complete, the mail application places it into a file system. The mailer program (or sender SMTP module) recovers the message from the file system, checks the addresses, establishes a reliable two-way communication link with a receiver mailer program, sends the message body, and terminates the link. This is all done lock-step, one step at a time.

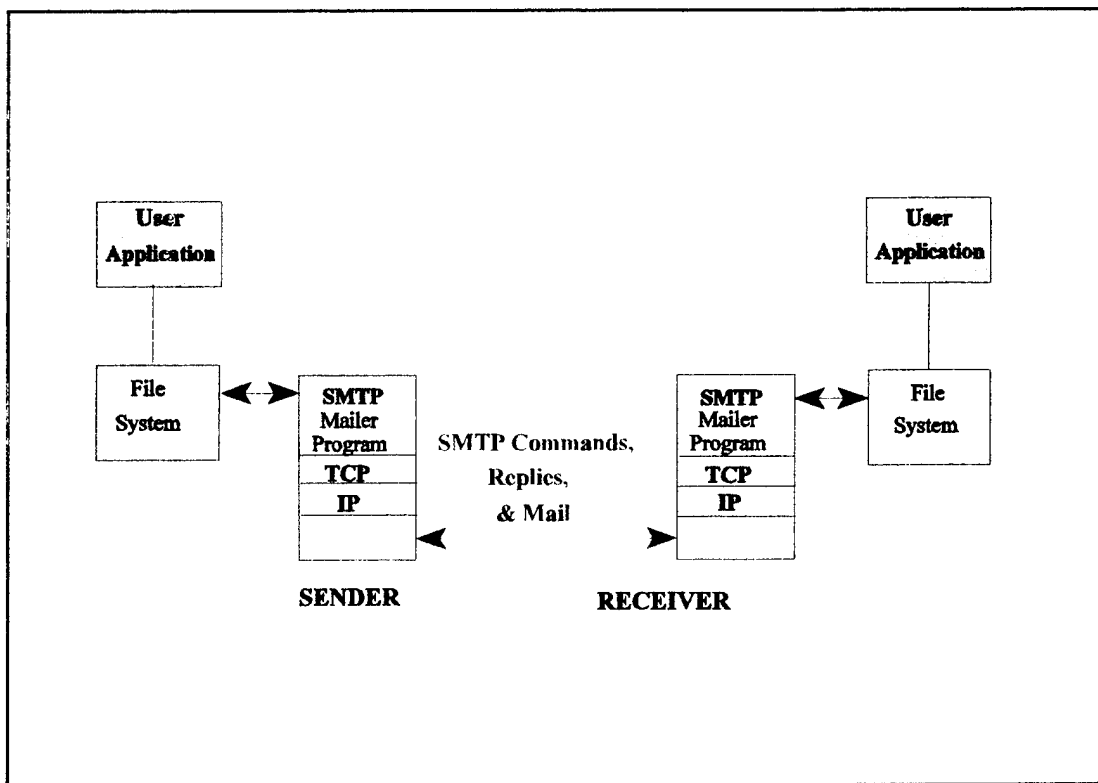


Figure 7.3 Simple Mail Transfer Protocol (Lynch 93)

administrator must keep close track of the state of the hosts in the domain and must have a complete understanding of the network.

3. Network News

Network news (USENET News) is one-to-many communication. It was motivated by a desire to move away from inefficient mailing lists and individual mail boxes as a form of broadcasting, to a system that loads and stores articles in a central database. A subscriber can get the news with a program designed to download it from a news server. Someone can post an article and anyone else can read it whenever they want. It is an electronic bulletin board. There are over 10,000 newsgroups on every topic conceivable (Cady 95).

Network News Transfer Protocol (NNTP) is used to transfer network news to a local system. It uses a reliable TCP data stream. A news server is a repository for news much as a POP server is a repository for mail. When a remote site wants to update the news in its repository, it downloads all the articles it does not have from subscribed newsgroups. This process is called a "news feed."

A full feed of all 10,000 newsgroups takes about 200 Megabytes of storage (Cady 95). The network manager can determine which newsgroups to receive for appropriateness and for conservation of storage. News items usually expire in 5 to 7 days to minimize the size of the mail feed (Cady 95). Figure 7.4 lists five steps to becoming a USENET site (Kamans 95). Other things that must be done by network staff include finding another news server administrator who is willing to provide a "news feed".

Some news service providers charge a fee for a news feed. The network manager must also ensure that there is enough disk space to keep all the articles. The POP server and NNTP server have similar functionalities and often it is convenient to place them on the same system (Lynch 95). The news application software recommended for Monterey BayNet work stations is called "WinVN NNTP" for PCs and "NewsWatcher" for Macs (Bigelow 95).

- Check that the benefits are worth the costs. Costs include time required to install and configure the software, and the cost of regular maintenance. Resources required are disk space (~5 Mb) for executables and on line resources, disk space up to 5400 Mb/month for storage of articles, and fees if the site is paying for a "feed".
- Find a site to provide a "news feed". Look for local sites at *newsgroup.comp.mail.maps* and ask the network administrator if they would be willing to provide a feed. Another approach would be to post a note on *News.admin.misc* with newsgroups. Last, if the two above don't work, subscribe under a commercial provider.
- Get the software. USENET software has three components: one component transports the news, another component stores the news on the local disk and expires old news, and the last component is a news reader for looking at the news.
- Install the software.
- Register the site. Some sites that are already in the Domain Name System and put their DNS name in a UUCP map entry as a alias for their site and use the DNS address rather than the UUCP host name in all mail and USENET postings. This way, both UUCP and DNS host can get mail and news to the site

Figure 7.4 Steps to become a USENET site (Kamans 95).

4. Network Time

The Internet is now a source for schools and organizations to maintain very accurate time information. Network Time Protocol (NTP) is a protocol built on top of UDP /IP that allows local clocks to be synchronized to radio and atomic clock references on the Internet (Cady 95). NTP (Version 3) is defined in Internet Standard STD 12 and RFC 1305. In 1972, national standard time was referenced to International Atomic Time, and is maintained using cesium-beam atomic clocks to an accuracy of 10^{-12} second. Primary (stratum 1) and secondary (stratum 2) time servers are connected using the Network Time Protocol (NTP) to reference time sources synchronized to the atomic clocks by wire and radio. The primary time servers also use NTP to compare their times with each other for error correction. This network of primary and secondary servers is configured in a hierarchy, with the secondary servers distributing their time via NTP to local net hosts (RFC 1305).

NTP is easy to implement and can be used to maintain local time to the millisecond. To do so, the network manager must decide on a machine that will be available at all times to be the time server. NTP imposes a very small load on a server, and also broadcast time on the local network. If there are multiple subnets, one server can be provided for each subnet. Second, the NTP software is obtained and installed on the machine. UCLA Time Services provides freeware that will allow Unix, PC, or Macintosh workstations to obtain accurate time, and in some cases receive continuous time synchronization traceable to National Institute of Standards and Technology's (NIST) atomic clocks in Colorado. It available at: <http://www.ucla.edu/campus/computing/time/>

Other primary (stratum 1) and secondary (stratum 2) NTP time servers are available for public access at <http://www.eecis.udel.edu/~mills/ntp/servers.html> . Each entry gives the host name, Internet address, approximate location and geographic coordinates (if available), synchronization source (stratum, type of radio or satellite receiver, host type), suggested service area, access policy (as notified) and contact name and e-mail address.

A client sends an NTP message to the server and processes the replies as received. Information included in the NTP message allows the client to determine the server time with respect to local time and adjust its internal clock accordingly.

5. World-Wide Web (WWW) Service

In a short number of years, the WWW has grown to a tremendous size and its popularity is responsible in part for the explosion in the growth of the Internet. WWW pages can appear like an electronic magazine or multimedia presentation. Fundamentally, the Internet can be considered as network connectivity infrastructure and the WWW can be considered as all the information content retrievable over the Internet. Figure 7.5 lists the steps subscribing sites can take to support the creation and storage of Web pages (Cady 95). Web pages have tremendous potential for students to be creative and demonstrate their progress to parents, friends and relatives at the same time.

CERN httpd is a full-featured hypertext server which can be used as a regular HTTP server. It is available at: <http://www.w3.org/hypertext/WWW/Daemon/>

- An http or "Web" server on the local network.
- Directories in the server organized to provide a location for storage of different types of files (images as .gif, .jpg, .mpg, sound files as .au, html files as http, etc.).
- Read-only or read-write file permissions to restrict users to files within specific directories.
- a link from the top level menu to a Web search server so that users can find materials out on the Web.
- Tools, utilities and graphics for use in constructing home pages.

Figure 7.5 Setting up a Web server (Cady 95).

6. Documentation and Training

Although it is up to subscribers to provide school-specific and organization-specific information, the Network Information Center (NIC) can provide generic Internet information that applies to everyone on Monterey BayNet. Some of the areas to cover include how to use *telnet*, *ftp*, and *e-mail*.

a. *telnet*

telnet provides the most basic kind of computer connectivity and is described in (RFC 854, 83). It allows a person to sit at one computer and use another remote computer, all as if they were sitting at a command-line terminal directly connected to the remote computer. This is called "virtual terminal access." HYTELNET is a collection of information about public *telnet* sites. It is designed to assist and give users access to all of the libraries, Free-nets, BBSs and other *telnet*-accessible information sites on the Internet. It is especially for those who access *telnet* from a Mac or an IBM

compatible personal computer. The *telnet* software recommended for Monterey BayNet is called "Trumptel" for PCs and "Telnet" for Macs (Bigelow 95). More information about *telnet* and HYTELNET is available on the World Wide Web at <http://hws3.hws.edu:9000/www/Telnet.html>

b. *ftp* (file transfer protocol)

As its name implies, *ftp* is used to transfer files from one computer to another. Sites that make their files available for public access are called "anonymous *ftp*" sites, so named because "anonymous" is the user name that permits access. Web browsers like Netscape and Mosaic can get files from anonymous *ftp* sites by setting up a link on a Web page. Selecting that link transfers the file to a local computer.

archie is an *ftp* search program. It searches through lists of files at anonymous sites, looking for a word or phrase specified at the beginning of the search. *archie* can be also used through the Web. A Web page is returned with *ftp* links to directories or files.

The *ftp* software recommended for Monterey BayNet is called "*ftp*" for PCs and "Fetch" for Macs. The *ftp* search program for PCs is called "Archie" and "Anarchie" for Macs (Bigelow 95). More information about *ftp* and *archie* is available on the World-Wide Web at: <http://hws3.hws.edu:9000/www/FTP.html>

c. *Mail*

Although the mechanics of Simple Mail Transport Protocol (SMTP) have been discussed previously, it is transparent to users. It is important that NIC staff provide

some information on how to use mail applications. The mail application software recommended for Monterey BayNet is called "Eudora" for both PCs and Macs (Bigelow 95). Eudora is really designed for single-user workstations. In multiple-user workstations, users can insert their own floppy with personal configuration settings and then start the Eudora mail application (Bigelow 95).

Eudora also supports the use of Multi-purpose Internet Mail Extensions (MIME). MIME became an Internet standard in 1992 and builds on the older e-mail standard by adding fields for mail message headers that describe new types of content and organization for messages. MIME allows mail messages to contain:

- Multiple objects in a single message.
- Character sets other than ASCII.
- Multi-font messages.
- Binary or application specific files.
- Images, audio, video and multimedia messages.

d. Other Network Information Center (NIC) Services

The "Help Desk" is a function of the NIC. Ideally, the NIC should be staffed by individuals knowledgeable on all aspects of the network, servers, information resources and ways to access them. NIC telephone numbers and e-mail addresses can be advertised at the school sites and organizations for ready access. A "Monterey BayNet Online Users Guide" needs to be written and can serve as ready source of information on network services and applications. A good example of an online users guide is one

assembled by the Australian Academic and Research Network (AARnet). It can be found on the WWW at <http://www.st.nepean.uws.edu.au/docs/aarnet/>.

It is important that the NIC implement and distribute a Monterey BayNet Acceptable Use Policy (AUP) so that users know when their use of network resources is consistent with the mission and goals of the network. Houston Independent School District in Houston, Texas has a large archive of material on Acceptable Use Policies and other legal information on the HISD Armadillo WWW Server at <http://chico.rice.edu/armadillo/Rice/Resources/acceptable.html>

In addition, example acceptable use policies for schools, businesses, and network service providers can be found at: <gopher://chico.rice.edu:1170/11/More/Acceptable> .

The NIC can provide a local network news group to distribute information concerning the changes in the network and new resources to subscribers. Electronic mail lists can be used for urgent messages.

NIC staff schedule training seminars and workshops on a regular basis. Training can be held periodically on recurring topics and also on new topics at the NIC sites (County Offices of Education) or NIC staff can conduct routine training visits to the school sites or organizations.

D. SUMMARY

From chapter five it was evident that the function of Network Operating Center with its sophisticated network management system and technical staff is responsible for optimizing the operation of Monterey BayNet. Conversely, the function of the Network

Information Center (NIC) with its training staff is responsible for optimum employment of Monterey BayNet. The NIC staff provides invaluable information to subscribers on connecting to the network, and on standard network services and protocols such as *e-mail, telnet, ftp, Network News, Network Time*. They also provide information on applications that access and employ these protocols. They provide direction on where to find information and how to use the many search tools such as "Archie" (*ftp*), "Hytelnet" (*telnet*), and the many WWW search engines. Last, NIC staff conduct training to help subscribing schools and organizations gain lasting practical experience at employment of network resources.

VIII. NETWORK OPERATIONS EXAMPLE CASES AND ANALYSIS

A. INTRODUCTION

Three cases are presented and described with emphasis on how they are managed and staffed. In addition to visiting the sites, information about each of these networks is available on the World-Wide Web at URLs listed in the Reference Section of this thesis.

B. EXAMPLE CASES

1. NASA Science Information (NSI) Operations

Information was provided by Jeanine Kamerdze, network operations manager of NSI. NSI operations is located at Ames Research Center (ARC) at Moffett Federal Air Station, Mountain View, California. There are over 250 end-site routers in the network, and over 100,000 terminal components beyond those routers. The point of demarcation for NSI network responsibility is at end-site routers which connect directly to the wide-area network (WAN) owned and maintained by NSI. The sites maintain all network components beyond the WAN routers (Figures 8.1 and 8.2).

a. Background

NSI was established in 1989 to provide an integrated communications infrastructure for the NASA scientific community. The DECnet-based "Space Physics Analysis Network (SPAN)" and the TCP/IP-based "NASA Science Network (NSN)" were merged at Ames Research Center in a single network called the NASA Science

NASA Science Internet

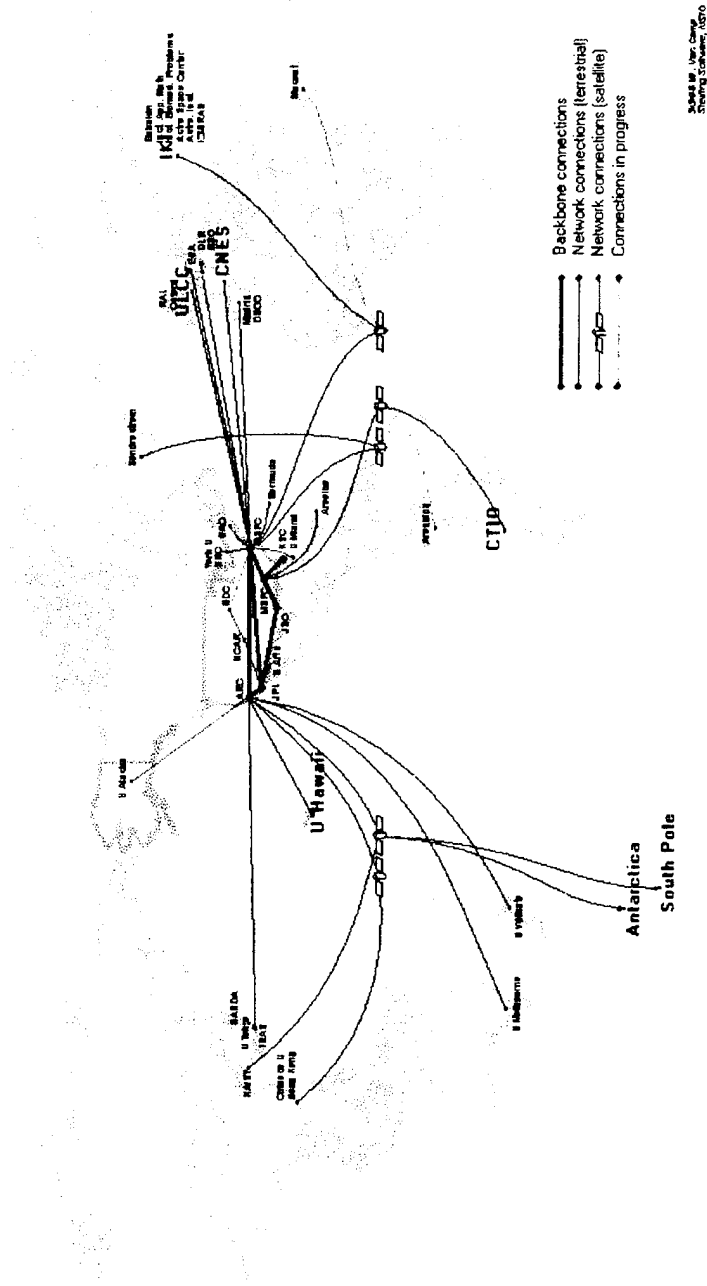


Figure 8.1 NASA Science Internet - World Network Map

Internet, or NSI. NSI is a high-speed, multiprotocol international network, that provides connectivity to six of the seven continents and will soon include Africa.

The mission of the NSI is to provide reliable and open access to NASA's widely distributed resources in support of NASA-funded projects. NSI provides a full range of networking services including network and data systems planning, network engineering, operations support, user support and outreach services. The main drivers of NSI's services are its users' requirements. Projects may require closed, secure networks or advanced types of applications requiring greater bandwidth (e.g. X-Windows, graphics and "telepresence" remote control of instruments).

NSI connects with the National Science Foundation Network (NSFnet), Bay Area Regional Research Network (BARRNet) and other federal agency networks. NSI cooperates with government, academic, and commercial organizations to improve interoperability and expedite migration to open systems and protocols (NASA Science Internet 94). Of particular interest to Monterey BayNet is NASA's strong commitment to K-12 Internetworking (Hodas 95). More Information is available at <http://quest.arc.nasa.gov/>

b. Network Description

The NSI backbone consists of a trunk with four parallel T1 lines traversing the nation and forming a ring with nodes at Ames Research Center (ARC), Goddard Space Flight Center (GSFC), Marshall Space Flight Center (MSFC), Johnson Space Flight Center (JSFC), and the Jet Propulsion Laboratory (JPL) in Pasadena, California (Fig. 8.2).

[illegible]

060825W . V IN CAMP
SHOOTING SCENE. AIS/O

Two network protocols are routed: IP and DECnet. These protocols are determined by subscriber requirements, with some subscribers requiring DECnet and others requiring IP. NSI tentatively plans are to slowly phase over to IP alone, but this will depend on the rate that subscribers shift to IP. The routing protocol used is BGP4 (Border Gateway Protocol) with Classless Interdomain Routing (CIDR).

The NSI network management system is DEC Polycenter 300 running SNMP and DECnet network management protocols. The network management workstations operate on UNIX. Graphical user interfaces (GUI) were custom designed by the NSI network analysts using *perl* and X-windows. Some displays were designed for statistics viewing capabilities. A large wall-projected topology display includes color-coded components, line speeds, alarms and projected alarm descriptions.

An integrated database (SYBASE) is used to store site information, accounting information, router configuration information, trouble-ticket and other historical information. Map-based site displays include site equipment configurations, circuit identification, and technical contact names, addresses and telephone numbers.

Fault management policies include a Trouble Ticketing (ARS) Action Request, escalation notification status log, and direct voice communication with the affected site(s). The system has e-mail notification of managers that is activated on faults when certain preset thresholds are exceeded.

For accounting management, there are 3 schemas (link schema, contacts schema, and site schema) used to present accounting information on each subscriber and site.

Whenever new sites are added to the network, NSI manages the process with a systematic site development program called "Facilities and Asset Management".

This breaks the task of incorporating each new site into four management stages:

- Requirements - obtain and define the user requirements. This includes line capacity, redundancy, uses of the link, etc.
- Engineering - design a solution to meet the user requirements. Hardware, software, protocols, media are selected.
- Provisioning - implementing the engineering solution. Addresses are assigned, routers are configured and transported to the remote site, connections are established.
- Operations - maintain the engineering solution. Performance and operation is monitored continuously.

This system facilitates smooth and complete incorporation of new sites. Training of newly subscribing site personnel is offered by NASA staff and an 800 toll-free number to NSI operations is provided for site support.

c. Staffing

NSI Operations maintains a staff of 9. The breakdown is:

- Network Manager (1)
- Network Operations Manager (1)
- Network Analysts (7)

The weekly calendar, with 7 network analysts (labeled a through g), is manned 24 hours daily, and seven days a week. A sample work schedule for 7 persons appears below:

| | SUN | MON | TUES | WEDS | THURS | FRI | SAT |
|------------------|-------|--------|---------|---------|---------|--------|-------|
| MID 00-08 | 1 (a) | 1 (a) | 2 (ab) | 2 (ab) | 2 (ab) | 1 (b) | 1 (b) |
| DAY 08-16 | 1 (c) | 2 (cd) | 3 (cde) | 3 (cde) | 3 (cde) | 2 (de) | 1 (e) |
| EVE 16-24 | 1 (f) | 1 (f) | 2 (fg) | 2 (fg) | 2 (fg) | 1 (g) | 1 (g) |

2. California State University Network (CSU NET)

Information on CSUnet was provided by Mike Marcinkevicz, network engineering manager, and Jim Patterson, network engineer of CSUnet operations. CSUnet network management center is located in Los Alamitos, California. There are over 250 end site routers in the network, with over 100,000 terminal components beyond those routers. Subscribing sites have custodial and maintenance responsibility for routers and other components that connect to the network.

a. Background

CSUnet is the computer network of the California State University system. In addition to 22 Cal State campuses, other CSUnet subscribers include local community colleges and school district offices within California. CSUnet provides a number of services depending on the needs of the subscribing site. CSUnet offers connectivity to the Internet and common services like email and gopher. Primary services and sites state-wide provide CSUnet access.

b. Network Description

The CSUnet backbone consists of two distinct components. One component consists of a state-wide network of dedicated leased lines accessed at the T1 capacity from subscribing sites (most of the 'original' CSU campuses) through Stratacom multiplexers. The other component consists of a TCP/IP network interconnected using Pacific Bell (PacBell) Telephone Company as connection provider. Routers are located at the subscribing sites. The two networks are connected so that Internet service is provided into the Stratacom network by MCI through a Cisco 7000 router.

Three network protocols are routed: IP, DECnet, and AppleTalk. These protocols are determined by subscriber requirements. Routing protocols are RIP (Routing Information Protocol), IGRP (Interior Routing Gateway Protocol), and BGP4 (Border Gateway Protocol) with Classless Interdomain Routing (CIDR).

CSUnet uses two different network management systems for the two different networks. The network management system for the Stratacom network is StrataView Plus and runs on a UNIX-based DEC 3200 workstation. For the TCP/IP

network, the network management system is SunNet Manager enhanced with Cisco Works, running on a SUN workstation. Network management protocols are SNMP for the TCP/IP network, and a Stratacom proprietary management protocol for the Stratacom network. A topological Stratacom network display is available for the Stratacom network that includes color-coded components, line speeds and alarms.

Information storage and retrieval is provide using "Filemaker Pro - Macintosh Server" by Apple. Trouble Tickets, accounting information, router configuration information, subscribing site and other historical information are entered manually. Fault management policies include trouble ticket generation and direct voice communication with the affected site(s).

Although CSUnet is part of the California State University system, CSUnet also serves many local community colleges and school district offices within California. CSUnet offers Internet services for these subscribers for a contracted fee based on line capacity. Limited training support is offered to new sites.

c. Staffing

CSUnet operations maintains a network staff of 11. The breakdown is:

- Network Manager (1)
- Network Operations Manager (1)
- Network Engineering Manager (1)
- Network engineers (2)
- Computer technicians (6)

CSUnet is monitored 24 hours daily, and seven days a week. The network management

center is manned during the day shift (7:00 am - 4:00 pm) and swing shift (4:00 pm - 12:00 am). The network is monitored by computer technicians on the mid shift (12:00 am - 7:00 am).

3. Energy Sciences Network (ESnet)

Information was provided by Tony Hain, associate network manager of ESnet. ESnet operations is located in the National Energy Research Supercomputer Center at Lawrence Livermore National Laboratory (LLNL) in Lawrence, California. There are over 55 end-site routers in the network, with over 100,000 terminal components beyond those routers (over 12,000 terminals are at LLNL alone). The point of demarcation for ESnet network responsibility is at end-site routers (called "border routers" by ESnet staff) that connect directly to the wide-area network (WAN) owned and maintained by ESnet. As with NSI, subscribing sites maintain all network components beyond the WAN routers (Figure 8.3).

a. Background

The Energy Sciences Network (ESnet) is a nationwide high performance network managed and funded by the U.S. Department of Energy Office of Energy Research (DOE / OER). Its mission is to support multiple programs and open scientific research. ESnet facilitates research collaboration by providing information access and distribution among scientists. It has served the energy research community almost exclusively since its inception. The primary use of ESnet is for five major DOE/OER programs: Applied Math, Basic Energy, Health and Environmental Research, High-Energy and Nuclear Physics, and Fusion Energy. The ESnet

"backbone" interconnects the local-area networks (LANs) of the subscribing sites (Energy Sciences Network 94).

In 1989 ESnet began initial deployment of a T1 (1.3 to 1.5 Mbps) circuit-based backbone. It became fully operational in 1990 with 19 major sites. Presently some ESnet sites are connected at speeds as high as 45 Mbps (T3). Connections to other scientific and educational locations are provided via the global Internet.

b. Network Description

ESnet is a high-capacity, high-performance network. The backbone consists of a full mesh ATM and conventional switched T3 (45 Mbps/sec) trunks (Figure 8.3). Nodes on the T3 ATM backbone include:

- Lawrence Livermore National Laboratory (LLNL),
- Fermi National Accelerator Lab (FNAL),
- Oak Ridge National Laboratory (ORNL),
- Los Alamos National Laboratory (LANL),
- Princeton Plasma Physics Laboratory (PPPL),
- General Atomics Fusion Group (GAC).

The conventionally switched T3 trunk connects Lawrence-Berkeley Laboratory (LBL) to LLNL, Sandia to LANL, and ANL to FNAL. Almost all of the remaining sites are connected to the T3 backbone by multiple T1's.

Presently, the link between the network operating center and PacBell is OC3 (155 Mbps) to support 3 T3's, and is being replaced with an OC 12 (622 Mbps) trunk to support 2 OC-3's & 6 T3's. In approximately 1 year, the OC 12 link will be replaced with an OC 48 (2500 Mbps) trunk. One reason for this large increase in

ESnet BACKBONE Early-1995

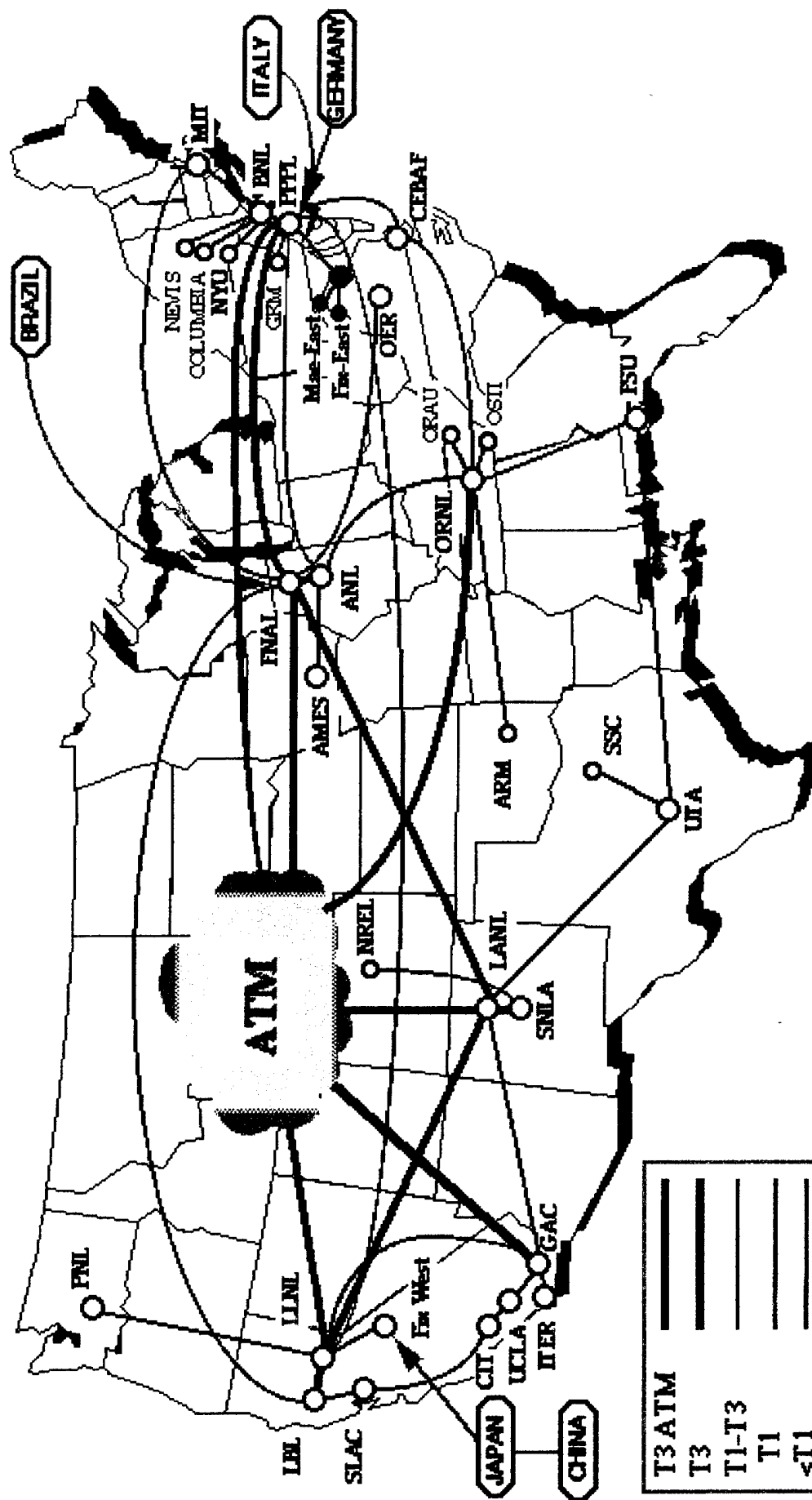


Figure 8.3 Energy Sciences Network (Esnet) - U.S. Network Map

11/10/84

capacity is shown in Figure 8.4. Network capacity is doubling about every 6 months which is consistent with global growth of the Internet at a sustained exponential rate of 15% per month.

ESnet connects to NSI, NSFnet and other networks on the Internet at nodes called "Fix East" and "Fix West". These nodes are two of the major communication traffic exchanges of the Internet. Additional interconnections with commercial Internet providers is done at the Network Access Point (NAP) facilities at Sprint (Pensauken, New Jersey), and MFS (Falls Church, Virginia.

Protocol (IP), DECnet Phase IV, and the Open Standards Interconnection

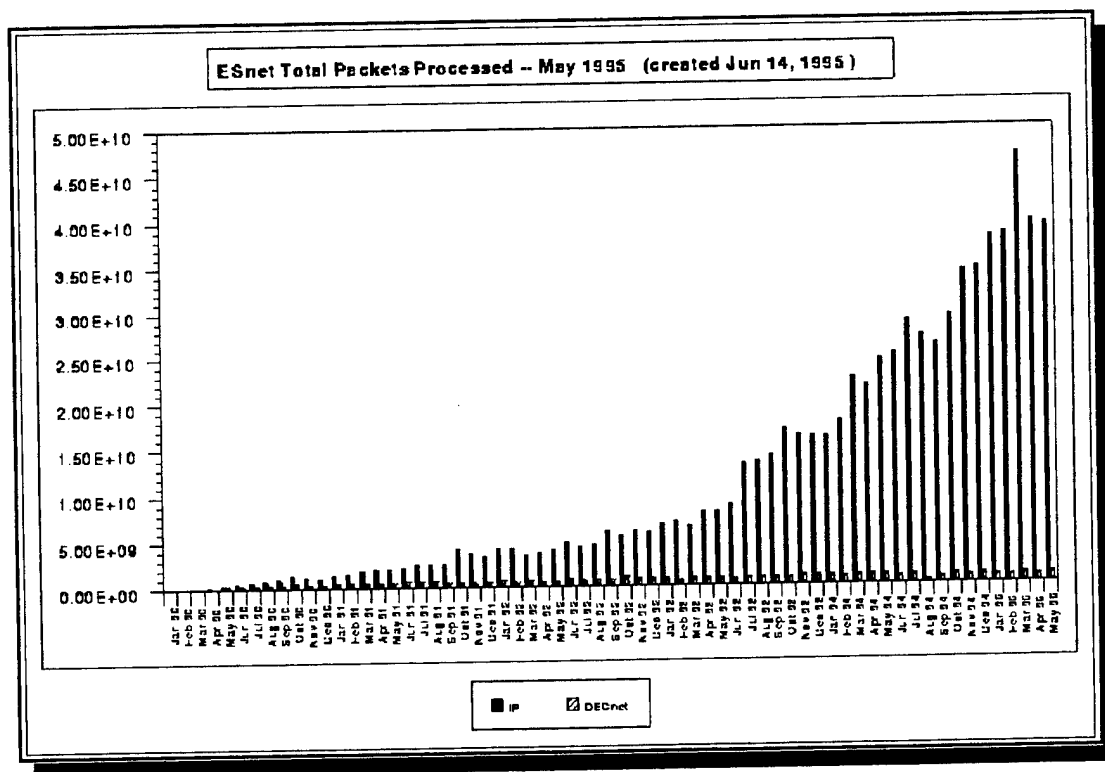


Figure 8.4 ESnet exponential growth (ESnet WWW page 95).

Multiple network layer protocols are supported by ESnet including the Internet ConnectionLess Network Protocol (OSI CLNP). These protocols are determined by subscriber requirements. Tentative plans are to phase over to IP alone in approximately 1 year, and route DECnet over IP. The routing protocol used is BGP4 (Border Gateway Protocol) with Classless Interdomain Routing (CIDR) for future scalability in addressing.

The ESnet network management system is DEC Polycenter running SNMP and DECnet network management protocols. The network management stations are X-windows based, with some workstations running UNIX and others running MicroSoft Windows NT (Figure 8.5). The dual operating system arrangement exploits the strengths of both operating systems while maintaining a common management application interface using X-windows. Graphical user interfaces (GUI) were custom designed by the ESnet network analysts. Some displays were custom developed for statistics viewing capabilities. A large wall-projected geographic-topological display of the Continental United States includes color coded components, line speeds, alarms and projected alarm descriptions.

Recently several popular network management systems were tested on the ESnet network for one week each. Cabletron SPECTRUM was selected as the best replacement available today for its displays. It will be supplemented by a separate statistics data program by SNMP Research, Inc. By splitting network management functionality between two separate products, better response time was demonstrated.

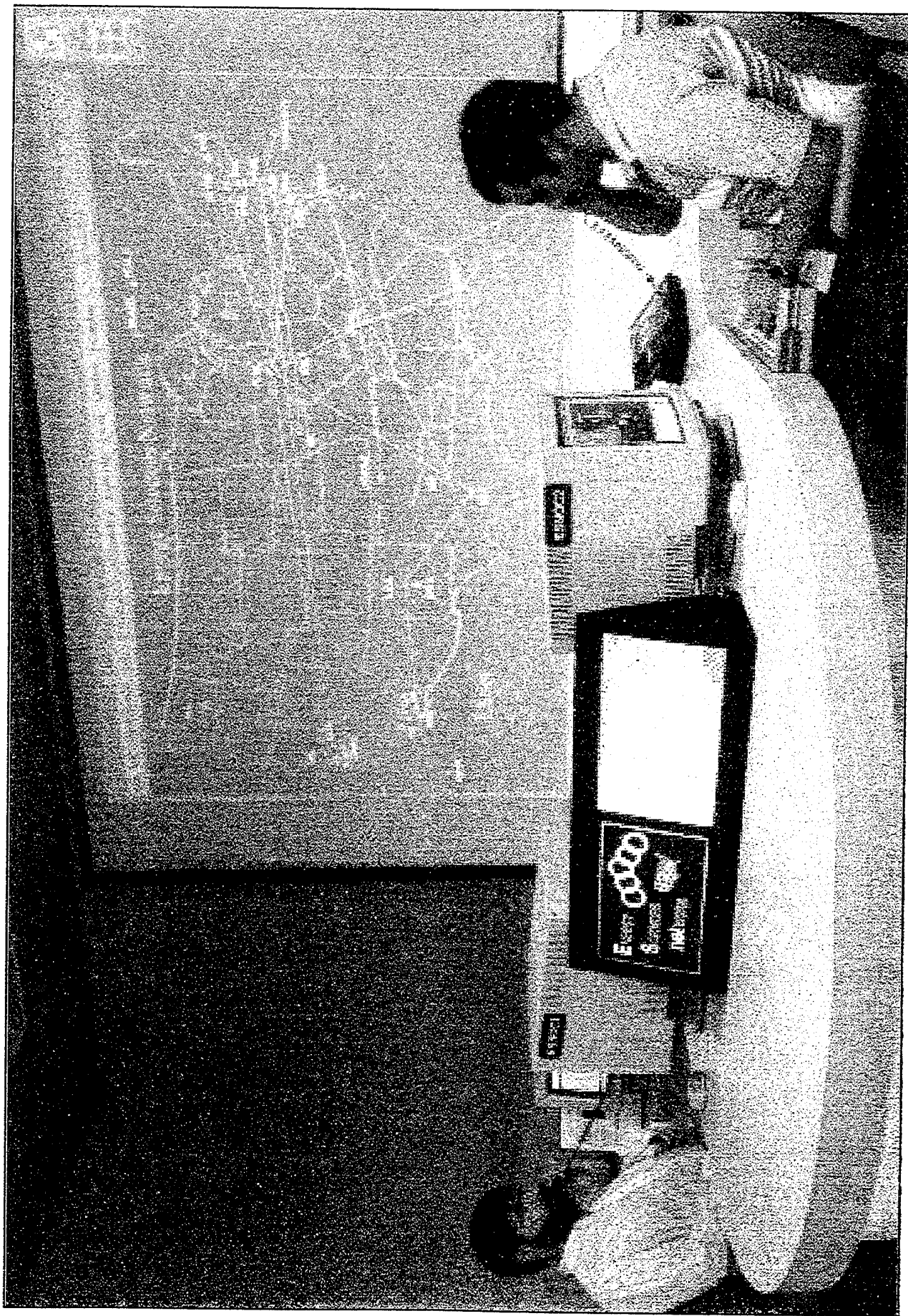


Figure 8.5 ESnet Network Operating Center

An integrated database (ORACLE) is used to store site information, accounting information, router configuration information, trouble-ticket and other historical information. Map-based site displays include site equipment configurations, circuit identification, technical contact names, addresses and telephone numbers.

Fault management policies include a trouble ticketing system, escalation notification, and direct voice communication with the affected site(s). The system has automatic remote paging of network operators and managers that is activated on faults when certain preset alarm thresholds are exceeded.

For accounting management, the centralized cost accounting approach is used and network expenses are covered by a budget set aside for ESnet. A chargeback (end-user accounting approach) is being considered due to cuts in government spending.

The ESnet operations staff maintains strict and exclusive control and access to their network. All routers are configured locally, tested and a government property sticker attached at ESnet before shipment to the site. All "border" routers belong to ESnet. Generally, sites want to control their own router interface with ESnet. Usually the site installs a router back-to-back with the ESnet operated router. This gives the local site manager control while maintaining a centrally operated and stable set of routers between sites.

Training for personnel at subscribing sites is the responsibility of the subscribers because training assets and network engineers are readily available at all of the sites.

c. Staffing

The staff of ESnet consists of the following:

- Network manager (1)
- Associate manager (1)
- Administrator (1)
- Computer Operators (10)
- Computer and network analysts (5)
- Information Specialists (5) (work with web servers, mail servers, build software and web pages)

The network operating center is manned 24 hours daily, 7 days a week. Monitoring responsibilities are distributed among staff personnel that run the supercomputer center as well as the network.

C. NETWORK MANAGEMENT SYSTEM ANALYSIS

A list of features used in evaluating network management systems is given in Figure 8.6 (Wilkinson and Capen 92). The last seven evaluation criteria in Figure 8.6 were added from a comprehensive executive summary generated in July 1994 by the University of Michigan Information Technology Division (ITD) Future Computing Environment (FCE) Monitoring Team. This team was formed in 1993 to evaluate Network Management Systems and is composed of 18 individuals from the medical, engineering, business, and information technology departments of the University.

1. Extended MIB(Management Information (data) Base)support - open ended MIB support (i.e. allows continued addition of features in the future)
2. Intuitive interface: GUI (Graphical User Interface)
3. Automatic discovery: System routinely polls the network to discover who's on the network.
4. Programmable events: Allows indications to change or actions to be taken when specified events occur.
5. Advanced Network Control: ability to control the operation of other major network components, shut down failing hubs, isolate faulty network segments, etc.
6. Object oriented management: Facilitates organization and function of user interface.
7. Custom Icons: Allows more granular representation of unique network components and enhances GUI capabilities.

Additional Items (University of Michigan 94):

8. Dependency Support: a network management systems ability to understand the relationship between all the devices on the network, so that when one of them fails, other devices downstream depending on that device for connectivity , are not seen as failing too.
9. Flexible Notification Methods: automatic e-mail alerts, pager alerts with programmable times for different methods of notification.
10. Support for trouble ticket systems: essential for troubleshooting and accounting.
11. Multi-vendor Integration: can manage components from different vendors, hubs routers, servers, switches, workstations.
12. Flexible access control: can specify access to different network resources (printers, servers, etc.) that a user can access.
13. Customized reports: tailoring reports to the needs of the organization.

Figure 8.6 Network Managment System Evaluation Criteria(Wilkinson and Capen 92)

Products evaluated in the 30 page executive summary with comments on key points were:

- Cabletron SPECTRUM - 1993 market share = 7.4%

Advantages:

- The only NMS to understand dependencies
- Access Control
- email, pager notification
- 1 year trial favorable results
- Object oriented
- X-windows and Command Line Interfaces
- Lower Price than others \$7,500

Disadvantages:

- Supported by few third party applications (enhancements)
- Slow auto-discovery
- No out of band management
- Awkward MIB browser
- Most complex of the products, needs extensive training to use

- Hewlett-Packard Open View - 1993 market share = 22.5%

Advantages:

- Supported by many third party applications (enhancements)
- Wide market use
- Industry standard base in NMS
- Easy to use GUI interface
- Easy to search database (SQL)

Disadvantages:

- Most Expensive ~ \$16,000 for end-user system
- No dependency heuristics
- Poor MIB browser
- Awkward to navigate GUI interface
- Redundant monitoring of devices shared on more than one network map
- Separate status and performance polling (longer to detect certain alerts)
- All interactions must use X-windows interface
- No text based alert screens(on-call persons can't dial-in for information)

- IBM NetView/6000 - 1993 market share (est.) ~ 15%

Advantages:

- Supported by many third party applications (enhancements)
- Wide market use
- Easy to use GUI interface
- Easy to search database (SQL)
- Improved Alarm filtering (fewer false alarms)

Disadvantages:

- Expensive ~ \$15,000
- No dependency heuristics
- Separate status and performance polling (longer to detect certain alerts)
- Redundant monitoring of devices shared on more than one network map
- All interactions must use X-windows interface
- No text based alert screens (no dial-in capacity for on-call persons)

- NetLabs DiMONS- 1993 market share = 9.0%

Advantages:

- Moderately Priced ~ \$7,500
- Graphically configurable(customize without programming)
- Powerful diagnostic capabilities for inexperienced users
- Conducts administrative inventory tasks through auto discovery
- E-mail and pager notifications

Disadvantages:

- No dependency heuristics
- Absence of application program interfaces - hard to program
- Unclear marketing future

- Sun SunNet Manager = 1993 market share = 35.9%

Advantages:

- First important UNIX based NMS
- Largest market share
- Most reasonable cost
- Distributed network management (polling by proxy consoles)
- Cooperative consoles allow multiple SNMs to share state information
- Dial-in access, email and pager alerts

Disadvantages:

- Requires a range of third party applications to be useful
- Runs only on a SPARC workstation
- No dependency heuristics
- Flat file database (relational database costs \$5,000 more)

A total of five network management systems were scored in this report. For the price, Cabletron SPECTRUM and Sun NetManager appear to offer the best capabilities. Of note is that ESnet personnel selected SPECTRUM as their main NMS after a 1 week evaluation each of SPECTRUM, OpenView and NetView. The latter two were sluggish for ESnet, which was subjectively attributed to excessive functionality at the expense of speed. CSUnet uses SunNet Manager for its TCP/IP network. NSI uses DEC Polycenter 300, which is not ranked among the "top 5" here. Other reports concur with the summaries above and can be found at the WWW location (mentioned earlier in chapter 2, section C) at:

<http://tampico.cso.uiuc.edu/~gresseley/netmgmt/>

D. SUMMARY

Three network cases were presented. Although they differ in many respects, there are also some things in common. All cases use TCP/IP protocol and SNMP network management protocol. All network managers stressed the importance of interoperability of network hardware and software and a desire to migrate their networks to a single network layer protocol, routing protocol and management protocol (SNMP).

An analysis of the top selling network management systems was also presented. Advantages and disadvantages were presented for each system against the evaluation criteria in Figure 8.6.

The most profound lesson to learn from network operating center staffing is that the relationship between the size of the network (i.e., number of routers for these

networks) and the number of staff is clearly nonlinear, with significant economy of scale as the network grows. Although the networks in these case studies are far larger than Monterey BayNet, many lessons learned by these larger organizations are applicable to regional networks.

IX. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The "Agenda of Education in California" mandates the use of telecommunication network technology for the K-12 educational mission. Other documents and regional efforts in the creation of Monterey BayNet support the same mission and envision MontereyBayNet as a reliable, high-capacity education and research network. To meet these mission objectives, Monterey BayNet must be managed.

Network management is the set of tasks and tools involved to *monitor* and *control* telecommunications networks. Many models exist to organize the tools and tasks of network management according to different views. Whatever model or combination of models is used, a successful final product will result in optimum efficiency and effectiveness of the network.

On a world scale, network management is increasing in importance with the rapid growth in telecommunications networks and the Internet. For a single K-12 network like Monterey BayNet, network management is essential if the network is to operate efficiently, to interoperate compatibly with other external networks, and to grow gracefully.

A network is composed of many "autonomous" individual components. Nevertheless, a network requires a manager to coordinate data flow among these

individual components just as a symphony requires a conductor to orchestrate individual musical instruments in concert.

There is tremendous potential to exploit the unprecedented access to vast quantities of information residing in the world's online information reserves. K-12 schools and other subscribers in Monterey BayNet must have a network that is responsive to two fundamental needs in preparing K-12 students and educators to meet the stiff, competitive environment of the information age.

- Monterey BayNet must have the capacity and reliability to perform over a broad range of information and data type and rates.
- Monterey BayNet must have enough reach to easily and conveniently access data at any and all available information resources in the National Information Infrastructure.

The first fundamental need involves Monterey BayNet's vital role as an educational "training aid" in teaching K-12 students and others in the use of network technology itself. The emphasis here is not on the information, but on the act of learning to use the network resource to obtain information. Put more simply, kids need a representative, reliable and adequate tool so they can learn how to use it.

The second fundamental need involves the ability of Monterey BayNet to access the information itself so that it can be used by K-12 students and educators in their studies. The "miracle" of the Internet is the vastness of germane information that it brings conveniently to the individual which was previously unavailable or hard to get.

Sustainability for Monterey BayNet involves continued usefulness in meeting the

needs requirements above. Monterey BayNet must be managed to continuously deliver and reliably meet these requirements 24 hours daily, seven days a week, equally to all subscribing sites. The sustainability of Monterey BayNet depends upon the reliability and consistency with which it meets user requirements .

B. RECOMMENDATIONS

Recommendations for regional action to assist the migration of Monterey BayNet to meet sustainability requirements are based on the numerous references and cases in this thesis. Consensus, practice and experience will further refine these recommendations.

1. Conformance to Standards

Hardware, software and network management systems **MUST** conform to standards before any other decision can logically be made (Stallings 93). Since the essence of network technology is interoperability, standards must be leveraged against present and future interoperability. Monterey BayNet has been designed with this concept as a primary goal in every decision in the design and construction of the network (Bigelow 95).

2. Network Management Protocol

The recommended network management protocol for Monterey BayNet is SNMPv2 (Simple Network Management Protocol, version 2). Reasons include:

- It can compatibly coexist with SNMP agents (interoperability).

- It corrects previous limitations of SNMP and retains all of its benefits.
- A large amount of operating experience has been gained in the use of SNMP.
- SNMP is designed as part of the Internet Protocol (IP) suite, an open standard and its widespread use makes it the *de facto* network management protocol (interoperability).
- SNMP is THE management protocol of choice for the largest and most complex networks including the NSI and ESnet. Concerns about effects of network size on the performance of SNMP appear to be exaggerated.
- SNMPv2 includes provisions for a secure network for present or future capability.

3. Network Management System (NMS)

Comparing the results of the network operating cases and analyses presented in Chapter VIII against the Evaluation Criteria in Figure 8.6, a case can be made to recommend Cabletron SPECTRUM based on performance and economy. Time permitting, however, a more detailed analysis is recommended. Prior to the purchase of a network management system for Monterey BayNet, it would be beneficial to do the following steps:

- Hire (or contract) a network manager with capability to evaluate NMS.
- Schedule Vendor demonstrations for each of the candidate products with the Monterey BayNet design committee and network manager. Include trouble ticketing systems, paging and e-mail notification.
- Request a trial run of the best candidates against each other on Monterey BayNet.

- Net design committee and network manager report the results and make final recommendation for purchase.

4. Staffing

The most striking item noted when looking at staffing requirements for the case Network Operating Centers(NOCs) and Network Information Centers(NICs), is that there is no clear relationship between the size of the networks and the staffing of the management center. In NSI, CSUnet and ESnet the exact number of end terminals is unknown. In fact , staffing is more governed by a need to be manned at certain times of the day and week than by network size.

In all of these cases, the WAN NOC was responsible for "border" routers and the subscribers were responsible for all downstream components. Bad WAN border routers are removed by subscribers and shipped to the NOC for repair, re-configuration, retest and shipment back to the site for installation. A spare configured router may be used for network service while the original is being repaired. Local expertise was available.

Monterey BayNet covers a small enough area that travel to any of the schools or other subscribing sites is possible by network personnel. However, expertise at most site locations is limited to nonexistent, so any trouble that cannot be corrected remotely by the NOC will require a site visit. This was not the case in the three networks examined in chapter 8. The level of experience with network and computing resources is much greater for users in the three cases. Monterey BayNet users will require considerably more training and user support functions.

In considering the above factors along with a projected size of Monterey BayNet of 200 routers in only a few years, the net design tiger team can consider the following as a baseline staffing recommendation:

- Network Manager (1) Supporting both counties at the NOC/NIC location.
- Network Service technicians (2 field workers), one per county.
- Help Desk (NIC), 2 shifts/day, 5 days/week, (4-6) two or three per county.

In selecting staffing, it is important to recognize that some leverage may be made by an aggressive training program of school teachers and other subscribers in reducing Help Desk demand. This requires travel and time away from the NIC. To date, a variety of tiger team proposals and efforts to provide volunteer training for teachers have only achieved modest results

It may be cost effective to have a third NIC person per county to conduct training and to cover for staff absences (e.g. sick days, vacations) School volunteers can also be used to augment paid staff.

5. Reports

Reports on network parameters will support the network manager and tiger team evaluations. Operational Reports are described in Section E.3 of chapter VI. The most useful are the daily status of active trouble tickets and a monthly report on the tally of tickets for the month. It is also useful to track number of tickets for individual components to record the number of failures over time. If reported failures are excessive, action may be taken to replace the component.

6. Accounting

Fixed end-user cost accounting is recommended as the chargeback mechanism for financing Monterey BayNet operations. Network costs are divided up fairly among subscribers and charged accordingly. There is also great economy of scale. As the same fixed cost is divided by an increasing number of subscribers, the cost of network operations is progressively lower per subscriber. This method costs the least of all accounting methods to administer.

Since the *primary* mission of Monterey BayNet is education of K-12 students, the execution of that mission is coordinated best by the County and District Offices of Education. Billing and collection functions ought be set up within the existing accounting framework of these organizations in order to eliminate any new accounting methods for schools.

Most importantly, fixed cost end-user accounting best supports the educational goals of Monterey BayNet for open unrestricted use by teachers and students.

C. RECOMMENDATIONS FOR FUTURE WORK

Most of the information in this document is ready for implementation.

Excellent opportunities exist to document the decisions and experience regarding the following:

- Operational Evaluation of Network Operating Systems - Selecting the NOC for Monterey BayNet.
- Implementing a NOC for Monterey BayNet - A K-12 Wide-Area Network.

- Planning, Staffing, and Implementing Network Services - Monterey BayNet Network Information Center.
- Monterey BayNet - Training Challenges in a New K-12 Wide-Area Network.
- Monterey BayNet Administration - Staffing and financing the cost of a K-12 WAN.

These areas are essential topics for ongoing lessons learned. It is likely that future theses might supplement tiger team efforts to analyze and document lessons learned in detail. It is clear that Monterey BayNet is producing an educational transformation that all school districts will eventually experience. This is a rich and invigorating area for hands-on evaluation and practical research.

D. SUMMARY

Long term sustainability of Monterey BayNet hinges on two key ideas:

- Efficient network operation (NOC): the coordination of data flow that only a carefully chosen network management system can provide.
- Effective network employment (NIC): the complete and optimum utilization of network resources by well-trained educators, students, and other subscribers.

Standards, network management protocols, a network management system, staffing, reports and accounting can achieve these goals and meet the needs of Monterey BayNet students and educators.

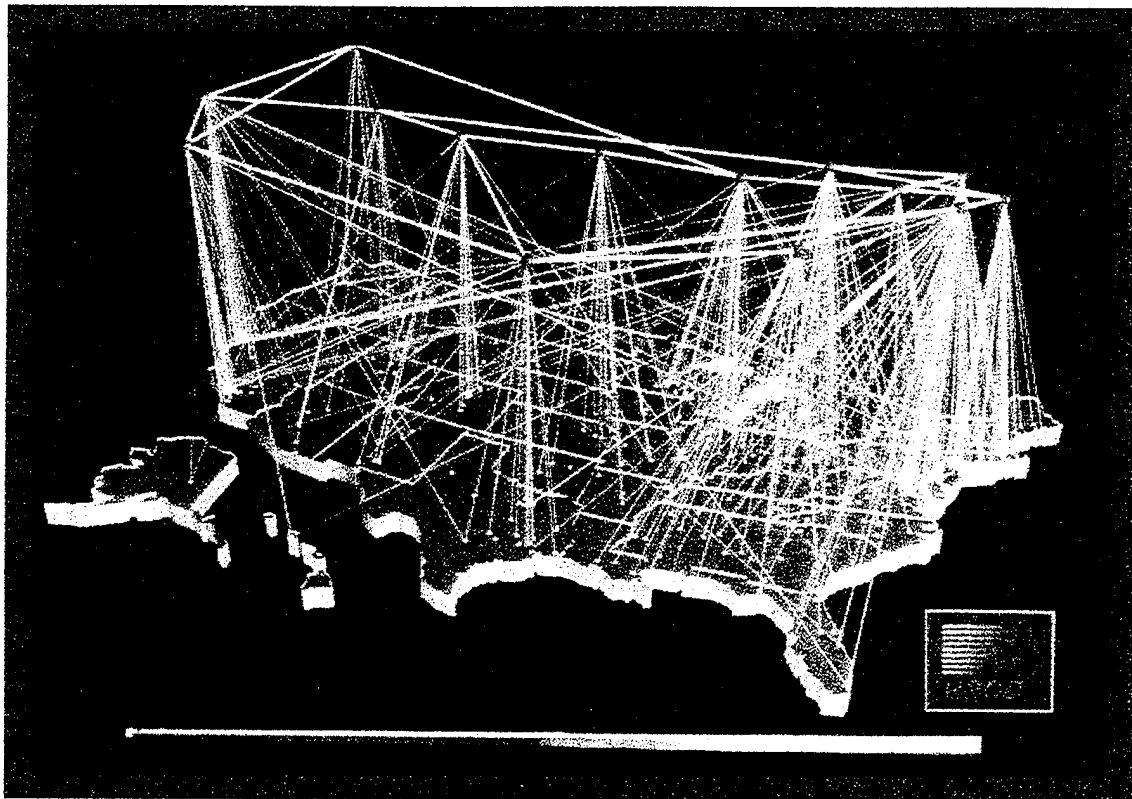


Figure 9.1 National Research and Education Network - Internet

LIST OF REFERENCES

Abraham, R., Russell, W., and Jas, F., *The Web Empowerment Book*, Springer-Verlag Publishers, Santa Clara California, 1994.

Aidarous, S., Proudfoot, D. and Dam, X., "Service Management in Intelligent Networks," *IEEE Network Magazine*, January 1990, pp. 18-24.

Aidarous, Salah and Prevakak, Thomas, *Telecommunications Network Management into the 21st Century: Techniques, Standards, Technologies and Applications*, IEEE Press, New York, 1994.

Albitz, Paul and Liu, Cricket, *DNS and BIND in a Nutshell*, O'Reilly & Associates, Sebastopol, California, 1993.

Amatzia, B., Chandna, A. and Warriar, U., "Network Management of TCP/IP Networks: Present and Future," *Journal of IEEE Networks*, vol. 4, no. 4, July 1990.

Atkinson, Marti, LAMBAY WWW Home Page, University of California Santa Cruz (UCSC), Santa Cruz, California, 1995. Available at:
<http://sapphire.cse.ucsc.edu/mb/index.html>

Bergeron, F., "The Success of DP Charge-Back Systems from a User's Perception," *Information and Management*, vol.10, no. 4, 1986, pp. 187-195.

Bigelow, Randall J., *Internetworking: Planning and Implementing a Wide-Area Network For K-12 Schools*, Master's Thesis, Naval Postgraduate School, Monterey, California, June 1995. Available at <http://www.stl.nps.navy.mil/~rjbigelo>

Birch, David, "An Information-Driven Approach to Network Security," *Second International Conference on Private Switching Systems and Networks*, IEE, London, United Kingdom, 1992.

Brutzman, Don, editor, *Initiative for Information Infrastructure & Linkage Applications (I²LA) Regional Network Design Tiger Team White Paper*, 22 Aug 1994. Available at ftp://taurus.cs.navy.mil/pub/i3la/i3la_net.txt and in PostScript format at ftp://taurus.cs.nps.navy.mil/pub/i3la/i3la_net.ps

Brutzman, Don, "Networked Ocean Science Research and Education, Monterey Bay, California," *Internet Society INET '95*, Honolulu, Hawaii, 26-30 June 1995. Available at <http://inet.nttam.com/HMP/PAPER/039/html/paper.html> and <ftp://taurus.cs.nps.navy.mil/pub/i3la/i3laisoc.html>

Cady, Glee H. and McGregor, Pat, *Mastering the Internet*, Sybex Inc., San Francisco, California, 1995.

California Department of Education, California K-12 Network Planning Unit, *Building the Future - K-12 Network Technology Planning Guide*, Sacramento, California, 1994. Available at the California Department of Education, 721 Capitol Mall, Sacramento, California 94244-2720, telephone (916) 657-5414.

California State University Network (CSUnet) World-Wide Web Page, "What is CSUnet?" August 1994. Available at: <http://www.csuchico.edu/computing/csunet.html>

December, John and Randall, Neil, *The World-Wide Web Unleashed*, 2nd edition, Sams Net Publishing, Indianapolis, Indiana, 1995.

Eastin, Delaine, "Agenda for Education in California," (poster) California State Superintendent of Public Instruction, Sacramento, California 1995.

Eckerson, W., "Net Management Traffic Can Sap Net Performance," *Network World*, May 4, 1992.

Eubanks, Steven, "Network User Guides", NASA- Lewis Research Center, Cleveland, Ohio, August 2, 1994, Available at http://netgopher.lerc.nasa.gov/Guides/guides_overview.html

Emery, James C., *Management Information Systems - The Critical Strategic Resource*, Oxford University Press, New York, 1987.

Fielding, Roy, Department of Information and Computer Science WWW page, "Country Codes," University of California, Irvine, California, July 1994. Available at <http://www.ics.uci.edu/WebSoft/wwwstat/country-codes.txt>

Freeman, Roger L., *Telecommunication Transmission Handbook*, 3rd edition, John Wiley and Sons, Incorporated, New York, 1991.

Gressley, Christine, Network Management Resources WWW page, Computing & Communications Services Office, University of Illinois at Urbana-Champaign, 1995. Available at <http://tampico.cso.uiuc.edu/~gressley/netmgmt/>

Held, Gilbert, *Network Management - Techniques, Tools, and Systems*, John Wiley and Sons, New York, 1992.

Heyne, Paul, *Microeconomics*, Macmillan College Publishing Company, New York, 1994, pp. 306-308.

Hodas, Steven, NASA's K-12 Internet Initiative, "Quest", WWW page, August 95,
Available at <http://quest.arc.nasa.gov/>

Hughes, Kevin, *Entering the World-Wide Web: A Guide to Cyberspace*, technical
report, Enterprise Integration Technologies, Palo Alto California, May 1994.
Available at <http://www.eit.com/web/www.guide/>

IBM Corporation, *AIX SystemView NetView/6000 USERS GUIDE, Version 2*, IBM
Publications, Research Triangle Park, North Carolina, 1993.

IBM Corporation, *AIX Trouble Ticket/6000 AT A GLANCE, Version 1.2 and 2.0*,
IBM Publications, Research Triangle Park, North Carolina, 1993.

IBM Corporation, *AIX Trouble Ticket/6000 USERS GUIDE, Version 1.2 and 2.0*,
IBM Publications, Research Triangle Park, North Carolina, 1993.

IBM, *High-Speed Networking Technology: An Introductory Survey*, International
Business Machines International Technical Support Center, Research Triangle Park,
North Carolina, 1993.

Joseph, Linda C., *World Link: An Internet Guide for Educators, Parents and Students*,
Greyden Press, Columbus, Ohio, 1995.

Kamans, Jonathan, and Lewis, Chris, "How to Become a USENET site," Academic
Consulting WWW home page, Houston, Texas, 22 August 1995. Available at
<http://www.academ.com/academ/nntp.html>

Kamerdze, Jeanine, personal interview, Network Operations Manager, NASA Science
Information Network (NSInet) Operations, Ames Research Center, Mountain View,
California, July 1995.

Keen, Peter and Cummins, J. Michael, *Networks in Action*, Wadsworth Publishing
Company, Belmont, California, 1994.

Krol, Ed, *The Whole Internet: User's Guide and Catalog*, 2nd edition, O'Reilly and
Associates Inc., Sebastapol, California, 1993.

Lambert, Paul A., "The Lowdown on Lower Layer Security Protocols," IEEE
Computer Society Press, Los Alamitos, California, 1990.

Lewis, Lundy, "A Case-Based Reasoning Approach to the Management of Faults in
Communications Networks," *IEEE Communications Magazine*, 1993, pp.114-120.

Lo, Chi-Chun, "An Expert Integrator for Communication Networks Management," *Proceedings: Sixteenth Conference on Local Computer Networks*, IEEE Computer Society Press, Los Alamitos, California, 1990, pp. 369-374.

Lynch, Daniel C. and Rose, Marshall T., *Internet System Handbook*, Addison-Wesley Publishing Company, Inc., Greenwich, Connecticut, 1993.

Milham, D. J., "British Telecom ONA-M," (Open Network Architecture for Management), *IEE Colloquium on Network Management and Signaling*, IEE, London, United Kingdom, 1992, pp. 4/1 - 4/3.

NASA Science Internet (NSI) World-Wide Web Page, "What is the NASA Science Internet?" June 1994. Available at <http://naic.nasa.gov/nsi/what-is-nsi.html>

"Network Time Protocol (NTP) at the University of Michigan," World-Wide Web page updated May 1995. Available at <http://www.umich.edu/~rsug/ntp/>

McKinney, Eric, "Matrix Information and Directory Service (MIDS)", World-Wide Web Page, August 1995, Available at <http://www.tic.com/mids/growth.html>

Moffett, Jonathan, "Network Security Management," *IEE Colloquium on Security and Networks*, digest No. 114, IEE, London, United Kingdom, 1990, pp. 4/1 - 4/7.

Pacific Bell, World-Wide Web home page San Francisco, California, 1995. Available at <http://www.pacbell.com>

Park, J.T., Choi, Y.W., Jung, J.W. and Sunwoo, J.S., "The Integration of OSI Network Management and TCP/IP Internet Management using SNMP," IEEE Computer Society Press, Los Alamitos, California, 1993, pp.145-154.

Parati, J., Parsons, M. and Yan, Gloria, "Service Pricing Strategies in an Internal Information System Services Organization with Captive Customers/Markets," *Proceedings of the 28th Annual Hawaiian International Conference on System Sciences*, IEEE, New York, 1995, pp. 504-513.

Potts, S.J., "Local Network Management", *IEE Colloquium on "Customer Access"*, Digest Number 038, IEE, London, United Kingdom, 1990, pp. 4/1-4/2.

Quinlan, Terrance A., *ADP Cost Accounting*, John Wiley and Sons, New York, 1989.

RFC 862, Postel, J., "Echo Protocol," May 1993 Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 821, Postel, J., "Simple Mail Transfer Protocol," August 1982, 58 pp.
Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 854, Postel, J. and Reynolds, J., "Telnet Protocol Specification," May 1983, 15 pp., Available at <http://www.internic.net/ds/dspg0intdoc.html>.

RFC 896, Nagle, J., "Congestion Control in TCP/IP Networks," January 1984, 9 pp.
Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 951, Croft, B. and Gilmore, J., "Bootstrap Protocol," September 1985, 12 pp.
Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 974, Partridge, C., "Mail Routing and the Domain Name System," January 1986, 7 pp., Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 977, Kantor, B. and Lapsley, P., "Network News Transfer Protocol," February 1986, 27 pp., Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1021, Partridge, C. and Trewitt, G., "High-Level Entity Management System HEMS," October 1987, 5pp. Available at
<http://www.internic.net/ds/dspg0intdoc.html>.

RFC 1034, Mockapetris, P., "Domain Names - Concepts and Facilities," November 1987, 55 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1035, Mockapetris, P., "Domain Names - Implementation and Specification," November 1987, 55 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1055, Romkey, J., "Nonstandard for transmission of IP datagrams over serial lines: SLIP," June 1988, 6 pp. Available at
<http://www.internic.net/ds/dspg0intdoc.html>

RFC 1123, Braden, R. "Requirements for Internet hosts - application and support," October 1989, 98 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1173, Van Bokkelen, J., "Responsibilities of Host and Network Managers - a Summary of Oral Tradition on the Internet," August 1990, 5 pp. Available at
<http://www.internic.net/ds/dspg0intdoc.html>

RFC 1180, Socolofsky, T. and Kale, C., "TCP/IP Tutorial," January 1991, 28 pp.
Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1156, McCloghrie, K. and Rose, M., "Management Information Base (MIB) for Network Management of TCP/IP based Internets," May 1990, 91 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1157, Schoffstall, M., Fedor, M., Davin, J. and Case, J., "A Simple Network Management Protocol (SNMP)," May 1990, 36 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1193, Ferrari, D., "Client Requirements for Real-Time Communication Services," November, 1990, 24 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1242, Bradner, S., "Benchmarking Terminology for Network Interconnection Devices," July 1991, 12 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1272, Mills, C., Hirsh, D. and Ruth, G., "Internet Accounting: Background," November 1991, 19 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1296, Lottor, M., "Internet Growth (1981-1991)," January 1992, 9 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1297, D. Johnson, "NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist (NOC TT Requirements)," January 1992, 12 pp., Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1305, Mills, D., "Network Time Protocol (Version 3) Specification, Implementation and Analysis," March 1992, 120 pp. Available at: <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1346, Jones, P., "Resource Allocation, Control, and Accounting for the Use of Network Resources," June 1992, 5 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1470, R. Enger and J. Reynolds, "FYI on a Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices," June 1993, 192 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1480, Cooper, A. and Postel, J., "The US Domain," June 1993, 47 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1578, Sellers, J., "FYI on Questions and Answers: Answers to Commonly Asked Primary and Secondary School Internet User Questions," Internet Engineering Task Force (IETF), Internet School Networking (ISN) Working Group, February 1994, 53 pp. Available at <http://ds.internic.net/rfc/rfc1578.txt>

RFC 1661, Simpson, W., "Point-to-Point Protocol (PPP)," July 1994, 54 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1709, Gargano, J. and Wasley, D., "K-12 Internetworking Guidelines," Internet Engineering Task Force (IETF), Internet School Networking (ISN) Working Group, December 1994, 26 pp. Available at <http://ds.internic.net/rfc/rfc1709.txt>

RFC 1718, Malkin, G., "The Tao of IETF - A Guide for New Attendees of the Internet Engineering Task Force," Internet Engineering Task Force (IETF), November 1994, 23 pp. Available at <http://ds.internic.net/rfc/rfc1718.txt>

RFC 1739, Kessler, G. and Shepard, S., "A Primer on Internet and TCP/IP Tools," December, 1994, 45 pp. Available at <http://www.internic.net/ds/dspg0intdoc.html>

RFC 1746, Manning, B. and Perkins, D., "Ways to Define User Expectations," Internet Engineering Task Force (IETF) working Group, December 1994, 18 pp. Available at <http://ds.internic.net/rfc/rfc1746.txt>

Rosen, Eric C. and Wittenbrink, Craig M., *Real-time Environmental Information Network & Analysis System (REINAS) WWW home page*, University of California Santa Cruz (UCSC), Santa Cruz, California, 1995. Available at <http://csl.cse.ucsc.edu/reinas.html>

Schatt, Stan, *Understanding Network Management, Strategies and Solutions*, Windcrest/McGraw-Hill, Harrisburg, Pennsylvania, 1993.

Sellers, J., "Internet School Networking (ISN) Charter, isn-charter home page," Internet Engineering Task Force (IETF), ISN Working Group, May 1995. Available at <http://www.ietf.cnri.reston.va.us/html/charters/isn-charter.html>

Stallings, William, *Data and Computer Communications*, Macmillan Publishing Company, New York, 1994.

Stallings, William, *SNMP, SNMPv2, and CMIP, The Practical Guide to Network Management Standards*, Addison-Wesley Publishing Company, Reading Massachusetts, 1993.

Sugarbroad, Ian, "An OSI-Based Interoperability Architecture for Managing Hybrid Networks," *IEEE Communications Magazine*, vol. 28 no. 3, New York, March 1990, pp. 61-69.

Tim, BL, and Frystyk, H. "About news servers and NNTP", WWW Page, July 1995
Available at
<http://www.w3.org/hypertext/WWW/LineMode/Defaults/AboutNewsServers.html>

Trepanier, Dennis, Buddenberg, Rex et al., *The Initiative for Information Infrastructure and Linkage Applications (I3LA) Network: Physical Configuration Team Project*, unpublished technical report, Naval Postgraduate School, Monterey California, April 1995.

University of Michigan, "Executive Summary - Future Computing Environment Monitoring Team, Final Report," technical report Information Technology Division (ITD) Future Computing Environment (FCE) Monitoring Team, July 1994. Available at <http://tampico.cso.uiuc.edu/~gressley/netmgmt/reviews/UofMichigan/ExecutiveSummary.html>

Wack, John P., and Carnahan, Lisa J., *Keeping Your Site Comfortably Secure - An introduction to Internet Firewalls*, technical report, National Institute of Standards and Technology, Washington, D.C. , 1994.

Walles, A., "Functional Description of Network Management," *Proceedings: Twelfth Annual International Phoenix Conference on Computers and Communications*, IEEE, New York, 1993, pp. 454-460.

Whittle, Jay, "Internet Standards WWW Page", 15 August 1995. Available at <http://www.isoc.org/standards/>

Wilkinson, S. and Capen, T., "Remote Control," *Corporate Computing*, October, 1992.

Willits, S.D. and Alley, L.R., "Capacity-Based Pricing Offers Viable Chargeback Alternative," *Data Management*, November 1985, pp. 23-28.

Yemini, Yechiam, "The OSI Network Management Model," *IEEE Communications Magazine*, New York, May 1993, pp. 20-29.

Appendix A - International Domain Names (Standard ISO 3166)

Fielding, Roy, Department of Information and Computer Science WWW Page, "Country Codes," University of California, Irvine, California, July 1994.

Available at <http://www.ics.uci.edu/WebSoft/wwwstat/country-codes.txt>

| | | | |
|----|------------------------|----|-----------------------------|
| AD | Andorra | CC | Cocos (Keeling) Islands |
| AE | United Arab Emirates | CF | Central African Republic |
| AF | Afghanistan | CG | Congo |
| AG | Antigua and Barbuda | CH | Switzerland |
| AI | Anguilla | CI | Cote D'Ivoire (Ivory Coast) |
| AL | Albania | CK | Cook Islands |
| AM | Armenia | CL | Chile |
| AN | Netherlands Antilles | CM | Cameroon |
| AO | Angola | CN | China |
| AQ | Antarctica | CO | Colombia |
| AR | Argentina | CR | Costa Rica |
| AS | American Samoa | CS | Czechoslovakia (former) |
| AT | Austria | CU | Cuba |
| AU | Australia | CV | Cape Verde |
| AW | Aruba | CX | Christmas Island |
| AZ | Azerbaijan | CY | Cyprus |
| BA | Bosnia and Herzegovina | CZ | Czech Republic |
| BB | Barbados | DE | Germany |
| BD | Bangladesh | DJ | Djibouti |
| BE | Belgium | DK | Denmark |
| BF | Burkina Faso | DM | Dominica |
| BG | Bulgaria | DO | Dominican Republic |
| BH | Bahrain | DZ | Algeria |
| BI | Burundi | EC | Ecuador |
| BJ | Benin | EE | Estonia |
| BM | Bermuda | EG | Egypt |
| BN | Brunei Darussalam | EH | Western Sahara |
| BO | Bolivia | ER | Eritrea |
| BR | Brazil | ES | Spain |
| BS | Bahamas | ET | Ethiopia |
| BT | Bhutan | FI | Finland |
| BV | Bouvet Island | FJ | Fiji |
| BW | Botswana | FK | Falkland Islands (Malvinas) |
| BY | Belarus | FM | Micronesia |
| BZ | Belize | FO | Faroe Islands |
| CA | Canada | FR | France |

| | | | |
|----|----------------------------|----|--------------------------|
| FX | France, Metropolitan | KP | Korea (North) |
| GA | Gabon | KR | Korea (South) |
| GB | Great Britain (UK) | KW | Kuwait |
| GD | Grenada | KY | Cayman Islands |
| GE | Georgia | KZ | Kazakhstan |
| GF | French Guiana | LA | Laos |
| GH | Ghana | LB | Lebanon |
| GI | Gibraltar | LC | Saint Lucia |
| GL | Greenland | LI | Liechtenstein |
| GM | Gambia | LK | Sri Lanka |
| GN | Guinea | LR | Liberia |
| GP | Guadeloupe | LS | Lesotho |
| GQ | Equatorial Guinea | LT | Lithuania |
| GR | Greece | LU | Luxembourg |
| GS | S.Georgia and Sandwich Is. | LV | Latvia |
| GT | Guatemala | LY | Libya |
| GU | Guam | MA | Morocco |
| GW | Guinea-Bissau | MC | Monaco |
| GY | Guyana | MD | Moldova |
| HK | Hong Kong | MG | Madagascar |
| HM | Heard and McDonald Islands | MH | Marshall Islands |
| HN | Honduras | MK | Macedonia |
| HR | Croatia (Hrvatska) | ML | Mali |
| HT | Haiti | MM | Myanmar |
| HU | Hungary | MN | Mongolia |
| ID | Indonesia | MO | Macau |
| IE | Ireland | MP | Northern Mariana Islands |
| IL | Israel | MQ | Martinique |
| IN | India | MR | Mauritania |
| IO | British Indian Ocean Terr. | MS | Montserrat |
| IQ | Iraq | MT | Malta |
| IR | Iran | MU | Mauritius |
| IS | Iceland | MV | Maldives |
| IT | Italy | MW | Malawi |
| JM | Jamaica | MX | Mexico |
| JO | Jordan | MY | Malaysia |
| JP | Japan | MZ | Mozambique |
| KE | Kenya | NA | Namibia |
| KG | Kyrgyzstan | NC | New Caledonia |
| KH | Cambodia | NE | Niger |
| KI | Kiribati | NF | Norfolk Island |
| KM | Comoros | NG | Nigeria |
| KN | Saint Kitts and Nevis | NI | Nicaragua |

| | | | |
|----|----------------------------|----|---------------------------|
| NL | Netherlands | SV | El Salvador |
| NO | Norway | SY | Syria |
| NP | Nepal | SZ | Swaziland |
| NR | Nauru | TC | Turks and Caicos Islands |
| NT | Neutral Zone | TD | Chad |
| NU | Niue | TF | French Southern Terr. |
| NZ | New Zealand (Aotearoa) | TG | Togo |
| OM | Oman | TH | Thailand |
| PA | Panama | TJ | Tajikistan |
| PE | Peru | TK | Tokelau |
| PF | French Polynesia | TM | Turkmenistan |
| PG | Papua New Guinea | TN | Tunisia |
| PH | Philippines | TO | Tonga |
| PK | Pakistan | TP | East Timor |
| PL | Poland | TR | Turkey |
| PM | St. Pierre and Miquelon | TT | Trinidad and Tobago |
| PN | Pitcairn | TV | Tuvalu |
| PR | Puerto Rico | TW | Taiwan |
| PT | Portugal | TZ | Tanzania |
| PW | Palau | UA | Ukraine |
| PY | Paraguay | UG | Uganda |
| QA | Qatar | UK | United Kingdom |
| RE | Reunion | UM | US Minor Outlying Islands |
| RO | Romania | US | United States |
| RU | Russian Federation | UY | Uruguay |
| RW | Rwanda | UZ | Uzbekistan |
| SA | Saudi Arabia | VA | Vatican City State |
| Sb | Solomon Islands | VC | Saint Vincent/Grenadines |
| SC | Seychelles | VE | Venezuela |
| SD | Sudan | VG | Virgin Islands (British) |
| SE | Sweden | VI | Virgin Islands (U.S.) |
| SG | Singapore | VN | Viet Nam |
| SH | St. Helena | VU | Vanuatu |
| SI | Slovenia | WF | Wallis and Futuna Islands |
| SJ | Svalbard and Jan Mayen Is. | WS | Samoa |
| SK | Slovak Republic | YE | Yemen |
| SL | Sierra Leone | YT | Mayotte |
| SM | San Marino | YU | Yugoslavia |
| SN | Senegal | ZA | South Africa |
| SO | Somalia | ZM | Zambia |
| SR | Suriname | ZR | Zaire |
| ST | Sao Tome and Principe | ZW | Zimbabwe |
| SU | USSR (former) | | |

INITIAL DISTRIBUTION LIST

| | | No. Copies |
|----|--|------------|
| 1. | Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145 | 2 |
| 2. | Library, Code 52 Naval Postgraduate School Monterey, California 93943-5101 | 2 |
| 3. | Dr. Hemant K. Bhargava, Code SM/Bh Naval Postgraduate School Monterey, California 93943-5101 | 1 |
| 4. | Dr. Don Brutzman, Code UW/Br Naval Postgraduate School Monterey, California 93943-5101 | 10 |
| 5. | Rex Buddenberg, Code SM/Bu Naval Postgraduate School Monterey, California 93943-5101 | 10 |
| 6. | Dr. Jim Eagle, Chair, Code UW Naval Postgraduate School Monterey, California 93943-5101 | 1 |
| 7. | Dr. Richard S. Elster, Provost Naval Postgraduate School Monterey, California 93943-5101 | 1 |
| 8. | Dr. James Emery Code 05 Naval Postgraduate School Monterey, California 93940 | 1 |

- 9 . CDR Robert Ellis, USN Code 37 1
 Naval Postgraduate School
 Monterey, California 93943-5101

10. Lt Tracey Emswiler, USN, Code SM 1
 1709 Yorktown St
 Omaha, NE 68123

11. Dr. Ruben Harris, Chair, Code SM/Ha 1
 Naval Postgraduate School
 Monterey, California 93943-5101

12. Dr. Ted Lewis, Chair, Code CS 1
 Naval Postgraduate School
 Monterey, California 93943-5101

13. Dr. G.M. Lundy, Code CS/Ln 1
 Naval Postgraduate School
 Monterey, California 93943-5101

14. Michael McCann, Code 51 1
 Director, Visualization Lab
 Naval Postgraduate School
 Monterey, California 93943-5101

15. Dave Norman, Code 51 1
 Director, W.R. Church Computer Center
 Naval Postgraduate School
 Monterey, California 93943-5101

16. Dr. Craig Rasmussen, Code MA/Ra 1
 Naval Postgraduate School
 Monterey, California 93943-5101

17. Dr. Maxine Reneker, Code 52 1
 Director, Dudley Knox Library
 Naval Postgraduate School
 Monterey, California 93943-5101

18. Dr. Myung W. Suh, Code SM/Su 1
 Naval Postgraduate School
 Monterey, California 93943-5101

- | | | |
|-----|--|----|
| 19. | LCDR Dennis Trepanier, USN, Code SM Naval Postgraduate School Monterey, California 93943-5101 | 1 |
| 20. | CAPT George Zolla, USN, Code 007 Naval Postgraduate School Monterey, California 93943-5101 | 1 |
| 21. | Dr. Michael J. Zyda, Code CS/Zk Naval Postgraduate School Monterey, California 93943-5101 | 1 |
| 22. | Arul K. Ananthanarayanan University of California Santa Cruz 225 Applied Sciences Bldg Santa Cruz, California 95064 | 1 |
| 23. | Cindy Atkins RD# 1 Box 177 Middlebury, Vermont 05753 | 1 |
| 24. | Larry Atkinson Center for Coastal Physical Oceanography Old Dominion University Norfolk, Virginia 23529 | 1 |
| 25. | Dr. Marti Atkinson University of California Santa Cruz CIS/CE Board Office 225 Applied Sciences Santa Cruz, California 95064 | 1 |
| 26. | Tierno S. Bah President and CEO AfriQ*Access, Inc. 12121 Turnstone Court Silver Spring, Maryland 20904 | 1 |
| 27. | Roland Baker Santa Cruz County Office of Education Media and Technology Services 809 Bay Avenue Capitola, California 95010 | 20 |

28. William Barr 1
County Superintendent of Schools
Monterey County Office of Education
PO Box 80851
Salinas, California 93912-0851
29. Jim R. Bellamy 1
System Design Consultant, Pacific Bell
5555 East Olive Avenue, Room A-400
Fresno, California 93762
30. Dr. Carl R. Berman, Jr 1
Office of the Provost
CSU Monterey Bay
100 Campus Center
Seaside, California 93955-8001
31. LT R. Jon Bigelow, USN 2
RD 3, Box 397
Middlebury, Vermont 05753
32. Roger L. Born 1
PO Box 1344
Monterey, California 93942
33. Bonnie Bracey 1
Christa McAuliffe Educator for the
National Foundation for the Improvement of Education
National Telecommunications and Information Administration
United States Department of Commerce
14th and Constitution Avenues, NW Room 4892
Washington, DC 20230
34. Dr. Peter Brewer 1
Executive Director
Monterey Bay Aquarium Research Institute
160 Central Ave
Pacific Grove, California 93950

- | | | |
|-----|---|---|
| 35. | Bill Brutzman 3 South Kingman Road South Orange, New Jersey 07079 | 1 |
| 36. | Jeff Bryant Monterey Bay Aquarium 886 Cannery Row Monterey, California 93940 | 1 |
| 37. | Carlos Burgos NASA Science Internet Mail Stop 233-8 Moffett Field, California 94035 | 1 |
| 38. | Fred Cohn Deputy to the City Manager City of Monterey City Hall Monterey, California 93940 | 1 |
| 39. | Coco Conn Interactive Communities Co-chair Digital Circus Productions SIGGRAPH 95 2207 Willetta Avenue Los Angeles, California 90068 | 1 |
| 40. | Dr. Tom Defanti Electronic Visualization Laboratory University of Illinois at Chicago, MC 154 851 S. Morgan St., Room 1120 Chicago, Illinois 60607-7053 | 1 |
| 41. | Honorable Sam Farr U.S. House of Representatives 1117 Longworth House Office Building Washington, D.C. 20515 | 1 |
| 42. | Elizabeth Fraser The Peck School 247 South Street Morristown, New Jersey 07960-7381 | 1 |

- | | | |
|-----|---|---|
| 43. | Dr. Nancy Giberson Santa Cruz County Office of Education 809 Bay Avenue Capitola, California 95010 | 2 |
| 44. | Dr. Peter Giles, President and CEO The San Jose Tech Museum of Innovation 145 West San Carlos Street San Jose, California 95113 | 1 |
| 45. | Bruce Gritton Monterey Bay Aquarium Research Institute (MBARI) 160 Central Ave Pacific Grove, California 93950 | 2 |
| 46. | Tony Hain Associate Network Manager Energy Sciences Network (ESnet) P.O. Box 5509 Mail Stop L-561 Livermore, California 94551 | 1 |
| 47. | Dr. Kathryn Lee Hanson Chief of Staff NII Activities Silicon Graphics, Inc. mail stop 002 2011 N. Shoreline Boulevard Mountain View, California 94043-1389 | 1 |
| 48. | Xin Hao Computing Center Institute of High Energy Physics Chinese Academy of Sciences 19 Yuquan Road Beijing 100039 | 1 |
| 49. | Mike Herbst Far West Laboratory 730 Harrison Street San Francisco, California 94107-1242 | 1 |

50. Eileen Hofmann 1
Center for Coastal Physical Oceanography
Old Dominion University
Norfolk, Virginia 23529

51. Jeanine Kamerdze 1
NASA Science Internet (NSI)
Mail Stop 233-8
Moffett Field, California 94035

52. LCDR James W. Kelly 1
Maintenance & Logistics Command Pacific (ts)
Coast Guard Island, Building 54a
Alameda, CA 94501-5100

53. Dr. Cathy Lascara 1
Center for Coastal Physical Oceanography
Old Dominion University
Norfolk, Virginia 23529

54. Syd Leung 2
Pacific Bell
2600 Camino Ramon, Room 35306
San Ramon, California 94105

55. Brian Lloyd 1
Lloyd Internetworking
3461 Robin Lane
Cameron Park, California 95682

56. Dr. Melanie Loots 1
Associate Director, National Center for Supercomputing Applications (NCSA)
4119 Beckman Institute, MC 251
University of Illinois at Urbana-Champaign
605 East Springfield Ave.
Champaign, Illinois 61820

57. Lora Lee Martin, Director 1
Director of Program and Policy Development
University of California, Santa Cruz
Santa Cruz, California 95064

- | | | |
|-----|---|----|
| 58. | Kam Matray Monterey Bay Technology Education Center, Monterey Peninsula Unified School District PO Box 1031 Monterey, California 93942-1031 | 2 |
| 59. | Chris May California State University, Monterey Bay 100 Campus Center Seaside, California 93955-8001 | 1 |
| 60. | Dr. James H. May California State University, Monterey Bay 100 Campus Center Seaside, California 93955-8001 | 1 |
| 61. | Ray McClain Moss Landing Marine Laboratories P.O. Box 450 Moss Landing, California 95039 | 1 |
| 62. | Honorable Henry Mello 1200 Aguajito Road. Monterey, California 93940 | 1 |
| 63. | Mike Mellon Monterey County Office of Education Instructional Resources and Technology PO Box 80851 Salinas, California 93912-0851 | 20 |
| 64. | Katie Muir Monterey Bay Aquarium 886 Cannery Row Monterey, California 93940 | 1 |
| 65. | Susan Netsorg Cabrillo College 6500 Soquel Drive Aptos, California 95003 | 1 |

- | | | |
|-----|--|---|
| 66. | Michael Newman Newman and Associates 24090 Summitwoods Drive Los Gatos, California 95030 | 1 |
| 67. | Julie Packard Director Monterey Bay Aquarium 886 Cannery Row Monterey, California 93940 | 1 |
| 68. | Richard Pearlman Technical Director, Knowledge Network 2150 Webster, Room 440 Oakland, California 94612 | 1 |
| 69. | Deborah Richards Industry Consultant, Pacific Bell 2460 North Main Street Salinas, California 93906 | 1 |
| 70. | Emily Routman Exhibit Developer, San Jose Tech Museum of Innovation 145 West San Carlos Street San Jose, California 95113 | 1 |
| 71. | Kathy Rutkowski Editor, NetTeach News 13102 Weather Vane Way Herndon, Virginia 22071-2944 | 1 |
| 72. | Jennifer Sellers NASA's K-12 Internet Initiative Sterling Software 700 13th Street, NW Suite 950 Washington, DC 20005 | 1 |
| 73. | Dr. Arthur St. George National Science Foundation 4201 Wilson Boulevard Arlington, Virginia 22230 | 1 |

74. Dr. Fred Siff, Associate Vice Chancellor
Communications and Technology Services
University of California, Santa Cruz
1156 High Street
Santa Cruz, California 95064 1
75. Dr. Horst Simon
Research Market Development Manager
Silicon Graphics, Inc.
mail stop 580
2011 N. Shoreline Boulevard
Mountain View, California 94043-1389 1
76. Diane Siri
County Superintendent of Schools
Santa Cruz County Office of Education
809 Bay Avenue
Capitola, California 95010 1
77. Dr. Larry Smarr
Director, National Center for Supercomputing Applications (NCSA)
155 Computing Applications Building, MC 476
University of Illinois at Urbana-Champaign
605 East Springfield
Champaign, Illinois 61820 1
78. Bradley R. Smith, Computer Facilities Manager
University of California, Santa Cruz
145 Applied Sciences Bldg
Santa Cruz, California 95064 1
79. Dr. Suresh Sridhar
Code SM/SR
Dept. of Systems Management
Naval Postgraduate School
Monterey, California 93940 1
80. LCDR Brian Steckler, USN
25381 Carmel Knolls Drive
Carmel, California 93923 1

- | | | |
|-----|--|---|
| 81. | David Stihler Monterey County Office of Education Instructional Resources and Technology PO Box 80851 Salinas, California 93912-0851 | 1 |
| 82. | Dr. Trish Stoddart University of California, Santa Cruz 211 Crown College Santa Cruz, California 95064 | 1 |
| 83. | Chris Taylor Director of Computing and Computer Resources (CCR) California State University, Monterey Bay 100 Campus Center Seaside, California 93955-8001 | 1 |
| 84. | Jim Warner Network Engineer, University of California Santa Cruz C A T S/Network & Telco Services 11 Communications Bldg Santa Cruz, California 95064 | 1 |
| 85. | David Warren Cabrillo College 6500 Soquel Drive Aptos, California 95003 | 1 |
| 86. | Steve Watkins University of California Santa Cruz Science Library Santa Cruz, California 95064 | 1 |
| 87. | Dr. Bruce Weaver Monterey Institute for Research in Astronomy (MIRA) Bin 568 Carmel Valley, California 93924 | 1 |
| 88. | Dr. Steve Webster Director of Education Monterey Bay Aquarium 886 Cannery Row Monterey, California 93940 | 1 |

- | | | |
|-----|--|---|
| 89. | Dr. Glen H. Wheless | 1 |
| | Center for Coastal Physical Oceanography | |
| | Old Dominion University | |
| | Norfolk, Virginia 23529 | |
| 90. | Marc W. Warshaw | 1 |
| | 124 White Oaks Lane | |
| | Carmel Valley, California 93924-9650 | |